alvarion®

Your Open WiMAX Choice

BreezeACCESS® and BreezeMAX™ Wi² Controllers

System Manual

SW Version 5.2
June 2008
P/N 215032

Legal Rights

The material contained herein is proprietary, privileged, and confidential and owned by Alvarion or its third party licensors. No disclosure thereof shall be made to third parties without the express written permission of Alvarion Ltd.

Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.

Trade Names

Alvarion®, BreezeCOM®, WALKair®, WALKnet®, BreezeNET®, BreezeACCESS®, BreezeMANAGE™, BreezeLINK®, BreezeConfig™, BreezeMAX™, AlvariSTAR™, AlvariCRAFT™, BreezeLITE™, MGW™, eMGW™, and/or other products and/or services referenced here in are either registered trademarks, trademarks or service marks of Alvarion Ltd.

All other names are or may be the trademarks of their respective owners.

Statement of Conditions

The information contained in this manual is subject to change without notice. Alvarion Ltd. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or equipment supplied with it.

Warranties and Disclaimers

All Alvarion Ltd. ("Alvarion") products purchased from Alvarion or through any of Alvarion's authorized resellers are subject to the following warranty and product liability terms and conditions.

Exclusive Warranty

(a) Alvarion warrants that the Product hardware it supplies and the tangible media on which any software is installed, under normal use and conditions, will be free from significant defects in materials and workmanship for a period of fourteen (14) months from the date of shipment of a given Product to Purchaser (the "Warranty Period"). Alvarion will, at its sole option and as Purchaser's sole remedy, repair or replace any defective Product in accordance with Alvarion' standard R&R procedure.

(b) With respect to the Firmware, Alvarion warrants the correct functionality according to the attached documentation, for a period of fourteen (14) month from invoice date (the "Warranty Period")". During the Warranty Period, Alvarion may release to its Customers firmware updates, which include additional performance improvements and/or bug fixes, upon availability (the "Warranty"). Bug fixes, temporary patches and/or workarounds may be supplied as Firmware updates.

Additional hardware, if required, to install or use Firmware updates must be purchased by the Customer. Alvarion will be obligated to support solely the two (2) most recent Software major releases.

ALVARION SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY PURCHASER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR IMPROPER TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

Disclaimer

(a) The Software is sold on an "AS IS" basis. Alvarion, its affiliates or its licensors MAKE NO WARRANTIES, WHATSOEVER, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. ALVARION SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT WITH RESPECT TO THE SOFTWARE. UNITS OF PRODUCT (INCLUDING ALL THE SOFTWARE) DELIVERED TO PURCHASER HEREUNDER ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED, MANUFACTURED OR INTENDED FOR USE OR RESALE IN APPLICATIONS WHERE THE FAILURE, MALFUNCTION OR INACCURACY OF PRODUCTS CARRIES A RISK OF DEATH OR BODILY INJURY OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE ("HIGH RISK ACTIVITIES"). HIGH RISK ACTIVITIES MAY INCLUDE, BUT ARE NOT LIMITED TO, USE AS PART OF ON-LINE CONTROL SYSTEMS IN HAZARDOUS ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS IN THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT MACHINES, WEAPONS SYSTEMS OR OTHER APPLICATIONS REPRESENTING A SIMILAR DEGREE OF POTENTIAL HAZARD. ALVARION SPECIFICALLY DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY OF FITNESS FOR HIGH RISK ACTIVITIES.

(b) PURCHASER'S SOLE REMEDY FOR BREACH OF THE EXPRESS WARRANTIES ABOVE SHALL BE REPLACEMENT OR REFUND OF THE PURCHASE PRICE AS SPECIFIED ABOVE, AT ALVARION'S OPTION. TO THE FULLEST EXTENT ALLOWED BY LAW, THE WARRANTIES AND REMEDIES SET FORTH IN THIS AGREEMENT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER

WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING BUT NOT LIMITED TO WARRANTIES, TERMS OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, SATISFACTORY QUALITY, CORRESPONDENCE WITH DESCRIPTION, NON-INFRINGEMENT, AND ACCURACY OF INFORMATION GENERATED. ALL OF WHICH ARE EXPRESSLY DISCLAIMED. ALVARION' WARRANTIES HEREIN RUN ONLY TO PURCHASER, AND ARE NOT EXTENDED TO ANY THIRD PARTIES. ALVARION NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

Limitation of Liability

(a) ALVARION SHALL NOT BE LIABLE TO THE PURCHASER OR TO ANY THIRD PARTY, FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES OF ANY KIND, WHETHER ARISING UNDER BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE AND WHETHER BASED ON THIS AGREEMENT OR OTHERWISE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

(b) TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE LIABILITY FOR DAMAGES HEREUNDER OF ALVARION OR ITS EMPLOYEES OR AGENTS EXCEED THE PURCHASE PRICE PAID FOR THE PRODUCT BY PURCHASER, NOR SHALL THE AGGREGATE LIABILITY FOR DAMAGES TO ALL PARTIES REGARDING ANY PRODUCT EXCEED THE PURCHASE PRICE PAID FOR THAT PRODUCT BY THAT PARTY (EXCEPT IN THE CASE OF A BREACH OF A PARTY'S CONFIDENTIALITY OBLIGATIONS).

Disposal of Electronic and Electrical Waste

Disposal of Electronic and Electrical Waste

Pursuant to the WEEE EU Directive electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Important Notice

This user manual is delivered subject to the following conditions and restrictions:

- This manual contains proprietary information belonging to Alvarion Ltd. Such information is supplied solely for the purpose of assisting properly authorized users of the respective Alvarion products.
- No part of its contents may be used for any other purpose, disclosed to any person or firm or reproduced by any means, electronic and mechanical, without the express prior written permission of Alvarion Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- The software described in this document is furnished under a license. The software may be used or copied only in accordance with the terms of that license.
- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.
- Alvarion Ltd. reserves the right to alter the equipment specifications and descriptions in this publication without prior notice. No part of this publication shall be deemed to be part of any contract or warranty unless specifically incorporated by reference into such contract or warranty.
- The information contained herein is merely descriptive in nature, and does not constitute an offer for the sale of the product described herein.
- Any changes or modifications of equipment, including opening of the equipment not expressly approved by Alvarion Ltd. will void equipment warranty and any repair thereafter shall be charged for. It could also void the user's authority to operate the equipment.

About This Guide

This guide describes the Wi^2 Controller Series for the Wi^2-CTRL-10, Wi^2-CTRL-40 and Wi^2-CTRL-200.

This guide comprises the following parts:

- Chapter 1 - Introduction
- Chapter 2 - MultiService Controller hardware
- Chapter 3 - Getting started
- Chapter 4 - Working with controlled APs
- Chapter 5 - Working with virtual networks
- Chapter 6 - Wireless mobility
- Chapter 7 - Network configuration
- Chapter 8 - Management
- Chapter 9 - Security
- Chapter 10 - User authentication
- Chapter 11 - Public/guest network access
- Chapter 12 - Local Mesh
- Chapter 13 - Working with autonomous APs
- Chapter 14 - Maintenance
- Appendix A - Regulatory information
- Appendix B - Resetting to factory defaults

- Appendix C - DHCP servers and Alvarion vendor classes

Contents

Chapter 1 - Introduction

Chapter 2 - Controller Hardware

Chapter 5 - Working with Virtual Networks

Chapter 6 - Wireless Mobility

Chapter 7 - Network Configuration

Chapter 8 - Management

Chapter 9 - Security

Chapter 10 - User Authentication

Chapter 11 - Public/Guest Network Access

Chapter 12 - Local Mesh

Chapter 13 - Working with Autonomous APs

Chapter 14 - Maintenance

Figures

1

Chapter 1 - Introduction

In This Chapter:

1.1 About this Guide

This guide explains how to install, configure, and operate the Wi² series MultiService Controllers and Wi² Controller Series MultiService Access Points operating in controlled mode. For information on the operation of APs in autonomous mode, consult the *MP Admin Guide*.

1.1.1 Products Covered

This guide covers the following products:

- Wi²-CTRL-10, Wi²-CTRL-40, Wi²-CTRL-200.
- Wi² AP (controlled mode plus basic autonomous mode information).

1.1.2 Important Terms

The following terms are used in this guide.

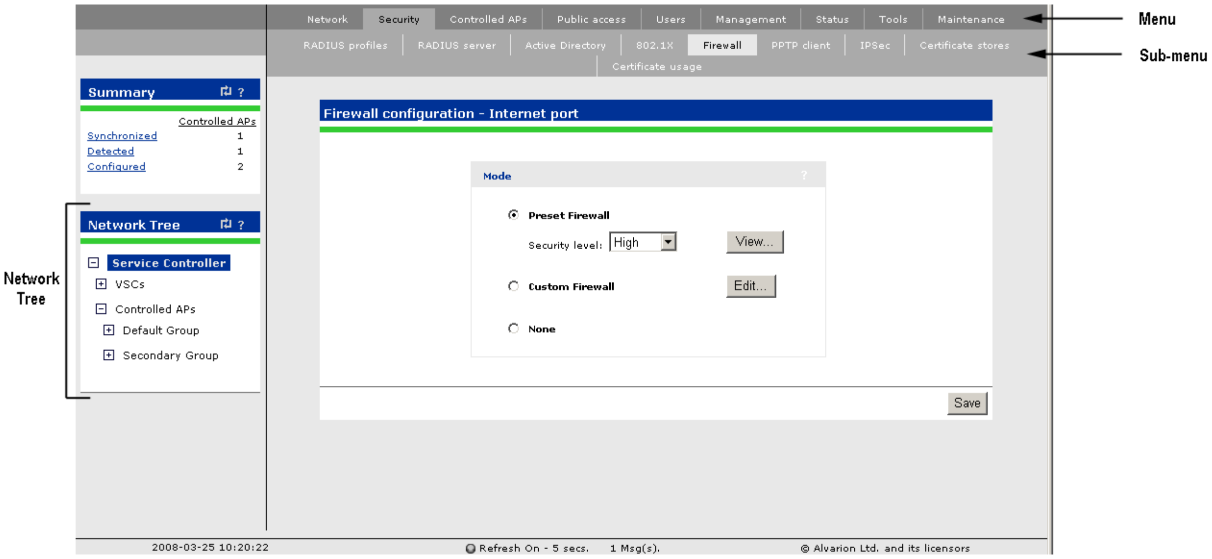
Term	Description
AP	Refers to Alvarion MultiService Access Points: Wi² AP. Non-Alvarion access points are identified as “third-party APs.” They do not support controlled mode.
Service controller	Refers to the Alvarion Wi² series of controllers, comprised of the Wi²-CTRL-10, Wi²-CTRL-40, and Wi²-CTRL-200.
Local mesh	In previous versions of the management tool and all former documentation, “local mesh” was known as “DWDS” (dynamic wireless distribution system).
AOS	Alvarion devices such as the Wi² series controllers and Wi² AP series APs run the Alvarion Operating System (AOS). References to specific versions of AOS are made in the form “at AOS x.x” as in “Wi² series controllers at AOS 5.2.”

1.1.3 Conventions

1.1.3.1 Management Tool

This guide uses specific syntax when directing you to interact with the management tool user interface. Refer to this image for identification of key user-interface elements and then the table below showing example directions:

maps



	Controlled APs
Synchronized	1
Detected	1
Configured	2

● Preset Firewall

Security level: High

○ Custom Firewall

○ None

2008-03-25 10:20:22 Refresh On - 5 secs. 1 Msg(s). © Alvarion Ltd. and its licensors

Figure 1-1: Sample Window

Example directions in this guide	What to do in the user interface
Select **Service Controller >> Security > Firewall**.	In the Network Tree select the **Service Controller** element, then on the main menu select **Security** and then select **Firewall** on the sub-menu. All elements to the left of the double angle brackets **>>** are found in the Network Tree.
Select **Service Controller > virtual networks >** [virtual network name] **>> Configuration**.	Expand the **Service Controller** branch (click its **+** symbol), expand the **virtual networks** branch, select a [virtual network name], and select **Configuration** on the main menu.
For **Password** specify **secret22**.	In the field **Password** enter the text **secret22** exactly as shown.

1.1.3.1.1 Commands and Program Listings

Monospaced text identifies commands, and program listings as follows:

Example	Description
`use-access-list`	Command name. Specify it as shown.
`ip_address`	Items in italics are parameters for which you must supply a value.
`ssl-certificate=`*`URL`*` [%s]`	Items enclosed in square brackets are optional. You can either include them or not. Do not include the brackets. In this example you can either include the “%s” or omit it.

Example	Description
`[ONE	TWO]`	Items separated by a vertical line indicate a choice. Specify only one of the items. Do not include the vertical line.

1.1.4 Warnings and Cautions

⚠ **WARNING**

Warnings must be heeded to avoid death or physical injury and to avoid hardware damage.

⚠ **CAUTION**

Cautions must be heeded to avoid loss of data or configuration information and to avoid improperly-configured networks.

1.1.4.1 Related Documentation

For information on related documentation, see the *Alvarion Ltd. Technical Documentation Road Map*, available on the *Alvarion Network Documentation CD* and for download on the Alvarion Ltd. extranet at http://extranet.alvarion.com.

1.2 The Alvarion Intelligent Mobility Solution

The Alvarion Intelligent Mobility Solution is a complete, optimized WLAN switching system for the deployment of secure, high-performance wireless networks.

The Alvarion Intelligent Mobility Solution makes it possible to leverage existing wired network security systems and authentication strategies to extend the services of a wired network infrastructure to wireless users. Key features include:

- High performance: Intelligent APs switch traffic at the network edge so that traffic flows directly from source to destination.
- Centralized management and control: Service controllers provide central management and control of APs making it easy to provide roaming, enforce consistent security and QoS policies, and automate AP configuration to minimize deployment and operation costs.
- Multi-layer security: Strong authentication, encryption, filtering, and VLAN tagging policies can be applied on a per-user basis at the network perimeter.
- Investment protection: Additional APs can be added to expand RF coverage as needs evolve.
- Consistent QoS: Ensures end-to-end performance and tailors QoS to meet the needs of all applications, such as guest Internet access, wireless telephony, and fixed mobile convergence.

1.2.1 Service Controllers

Service controllers are the central nervous system of the Alvarion Intelligent Mobility Solution, controlling the configuration, operation, and management of APs. Service controllers ensure consistent quality and security as users roam throughout the network. Supporting AP plug-and-play capabilities, service controllers simplify WLAN deployment and minimize network operation costs.

1.2.2 Intelligent APs

When deployed as part of the Alvarion Solution, Alvarion APs create a centrally-managed MultiService WLAN infrastructure with seamless roaming between APs. Designed for plug-and-play deployment, APs are controlled by service controllers, using an advanced protocol to automate configuration while ensuring continuous security and availability. APs are designed to satisfy the most demanding enterprise and service provider applications, while ensuring that configurations and software versions are synchronized across the WLAN.

APs offer support for the Local Mesh Protocol, an easy-to-configure wireless backhaul network, and the AP provides configurable QoS, security and a range of filtering capabilities.

APs offer versatile support for traditional stand-alone network topologies. They are easily configured for autonomous mode operation, still providing access to a rich set of features through local management interfaces.

1.2.3 Alvarion Operating System (AOS)

The Alvarion Operating System is embedded in all system components and creates a unified platform for consistent delivery of WLAN services. With AOS, a wide array of mobile applications can be delivered easily across a single WLAN infrastructure, including voice, data, and video services. Refer to “Product Summary” on page 12 for the list of available AOS options.

1.2.4 Centralized Management and Control

Service controllers provide centralized management and control of intelligent Alvarion APs distributed throughout a wireless zone, building, or campus, without the penalty of centralized switching. This significantly reduces backbone loads since user traffic is switched at the network edge and flows directly from source to destination. Service controllers handle only network control, management information, public access interface, and some authentication tasks, making them highly-scalable, cost-effective solutions.

1.2.4.1 Service Controller Managing Multiple APs Installed in Different Physical Locations

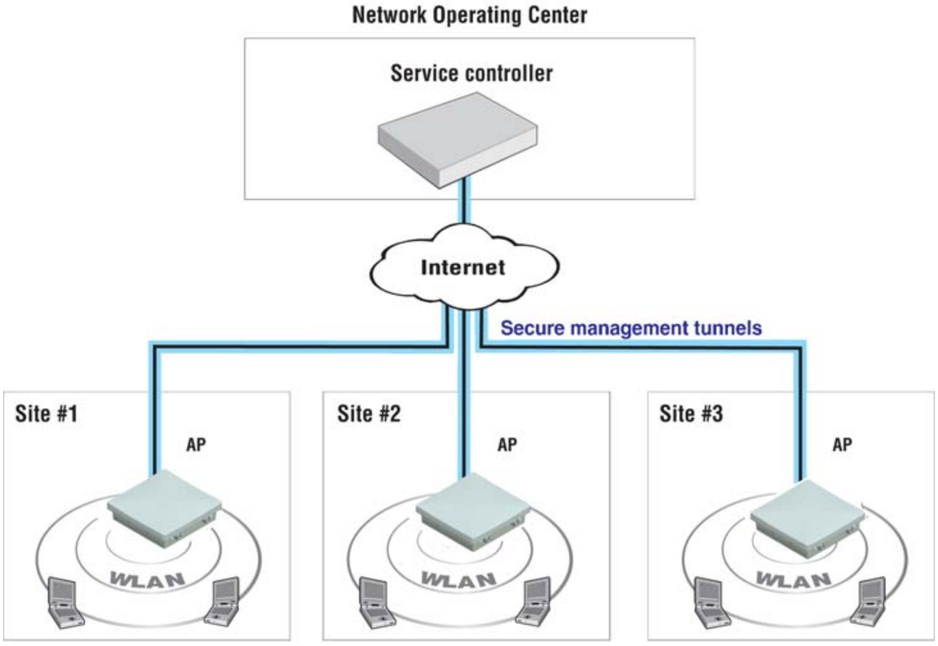


Figure 1-2: Service Controller Managing Multiple APs in Different Physical Locations

1.2.4.2 Service Controller Managing Multiple APs Installed in Different Areas at a Location

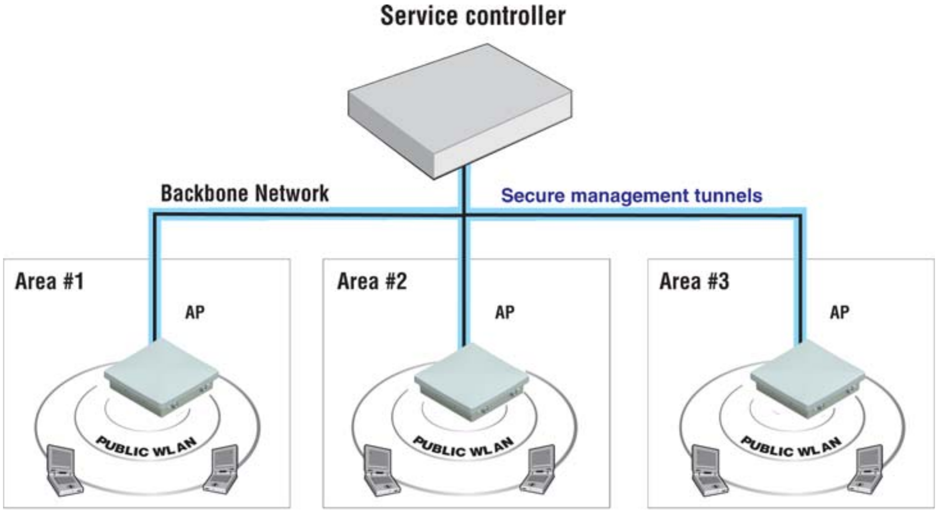


Figure 1-3: Service Controller Managing Multiple APs Installed in Different Areas at a Location

1.2.5 Simplified Configuration, Deployment, and Operation

For trouble-free deployment in geographically distributed networks, Alvarion service controllers automate discovery, authentication and configuration for a group of APs. Using standard dynamic look-up procedures, APs identify the service controller to which they are assigned. Mutual authentication using digital certificates assures security and eliminates the risk of rogue AP connectivity. Once authenticated, the service controller establishes an secure management tunnel for the exchange of configuration and control information with the AP.

The service controller provides centralized management for all APs. It eliminates time-consuming AP configuration, troubleshooting and maintenance tasks by providing a single management interface for the entire group of APs it manages. The service controller automates installation of AP software upgrades and ensures a consistent set of services are delivered throughout the network. All security, quality of service (QoS), and other policies can be centrally defined through the service controller's intuitive and secure web-based management tool.

1.2.6 Seamless Mobility

Alvarion service controllers include basic L2 (Layer 2) mobility support allowing wireless users to roam between Alvarion APs within the same subnet.

The optional Mobility license enhances basic wireless mobility by adding two separate features, WPA2 Opportunistic Key Caching and L3 Mobility.

1.2.6.1 WPA2 Opportunistic Key Caching

Using optimizations of 802.1X/802.11i authentication, WPA2 Opportunistic Key Caching enables a wireless client to perform a full RADIUS authentication once and then re-use those authentication credentials on each subsequent roam without the need to re-authenticate through RADIUS. The service controller caches keys on all possible APs to which roaming could occur so that a wireless user can roam between APs without incurring a full 802.1X RADIUS handshake delay.

WPA2 Opportunistic Key Caching provides secure and fast user authentication based on the WPA2 and 802.1X standards. It:

- Eliminates delays associated with reauthentication.
- Provides hand-offs in less than 50 milliseconds, as required for time-sensitive services such as voice.

- Preserves a user's RADIUS-assigned parameters such as security, QoS ,and VLAN, enabling a smooth transition of all services to which the user has access.

1.2.6.2 Layer 3 Mobility

Layer 3 (L3) mobility enables users to roam between APs that are connected to different subnets while maintaining their assigned IP address. L3 mobility enables a seamless wireless infrastructure to be deployed across a routed backbone network while delivering a consistent set of services to users, regardless of the subnets used for the underlying infrastructure. L3 mobility uses a unique technology set that eliminates the need for special client software required by some competing solutions.

1.2.7 Best-in-class Public/Guest Network Access Service

Designed to deliver the best possible user experience, the public/guest network access feature includes the Alvarion Zero Configuration Service Interface, which adapts to any client device IP address and web proxy settings, plus a customizable, web login page for easy sign-on.

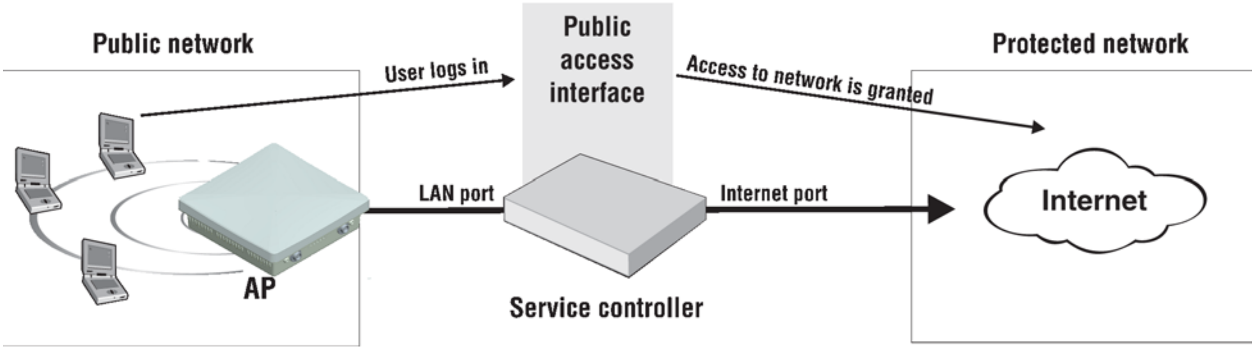


Figure 1-4: Best-in-class Public/Guest Network Access Service

To ensure seamless applications support, the public/guest network access feature uses Alvarion' advanced IP networking capabilities, including Adaptive NAT™, SMTP redirect, and DHCP services, providing transparent support for demanding applications, such as VPN tunneling, and email.

A rich feature set allows service providers to create a centrally-managed hotspot network. Support for a captive portal enables users to access special web content.

For your public access network, the service controller enables you to implement a variety of hotspot business models and back-end authentication and billing systems. Following are some of the possible scenarios:

- You have the flexibility to authenticate users locally or by referencing a centralized remote AAA server.
- You can collect session activity records that include elapsed time and bulk data transfers.
- You can redirect client stations to separate portal, AAA, and DHCP server destinations based on the user's location or associated SSID, enabling a range of service customization or wholesale service models. Alternatively, you can outsource these functions using the service controller's integrated support for leading third-party hotspot billing services.

High-performance Layer 2 encryption processing that can use WEP, WPA, and WPA2 (802.11i) protocols ensures privacy over the air. Client stations can authenticate using industry-standard 802.1x port authentication protocols or using their MAC addresses. The service controller supports a standard RADIUS AAA interface, which provides compatibility with popular enterprise authentication servers, including Microsoft Active Directory.

You can complement your WLAN security mechanisms and strengthen the network perimeter by configuring one or more virtual networks to apply Layer 2 or Layer 3 filtering and VLAN tagging.

In order to use the public access network, customers must successfully connect to the service controller through a wireless or wireline connection and be authenticated. This section covers all connectivity and authentication options that are configurable to support customers.

1.2.8 Superior Voice-Over-WLAN Support

With a service controller controlling its operation, the Alvarion Intelligent Mobility Solution delivers toll-quality voice services that leverage existing VoIP systems and extends telephony services to wireless phones. The Alvarion Solution features support for a wide range of standards-based and proprietary WLAN phones, including popular SpectraLink™ and Vocera™ handsets. WMM™ QoS mechanisms support emerging third-party phone clients and provide four levels of prioritization, enabling video and data services to be converged on the same WLAN.

Tested under rigorous conditions, the Alvarion Solution consistently delivers excellent voice performance, regardless of the amount of other traffic types that may also be using the network. WPA2 Opportunistic Key Caching ensures encrypted voice session hand-offs occur in under 50 milliseconds. With the flexibility of configurable powersave signals, handset battery performance is optimized, enabling the Alvarion Solution to improve handset recharge cycle time by as much as 50% over competing WLAN solutions.

1.2.9 Virtual Service Communities (VSCs)

The Alvarion Operating System (AOS) embedded in all service controllers works with other Alvarion components to create Virtual Service Communities (virtual networks)—discrete groups of network users with assigned service policies. AOS provides virtual network users with access to one or more applications that share a common set of QoS and security policies.

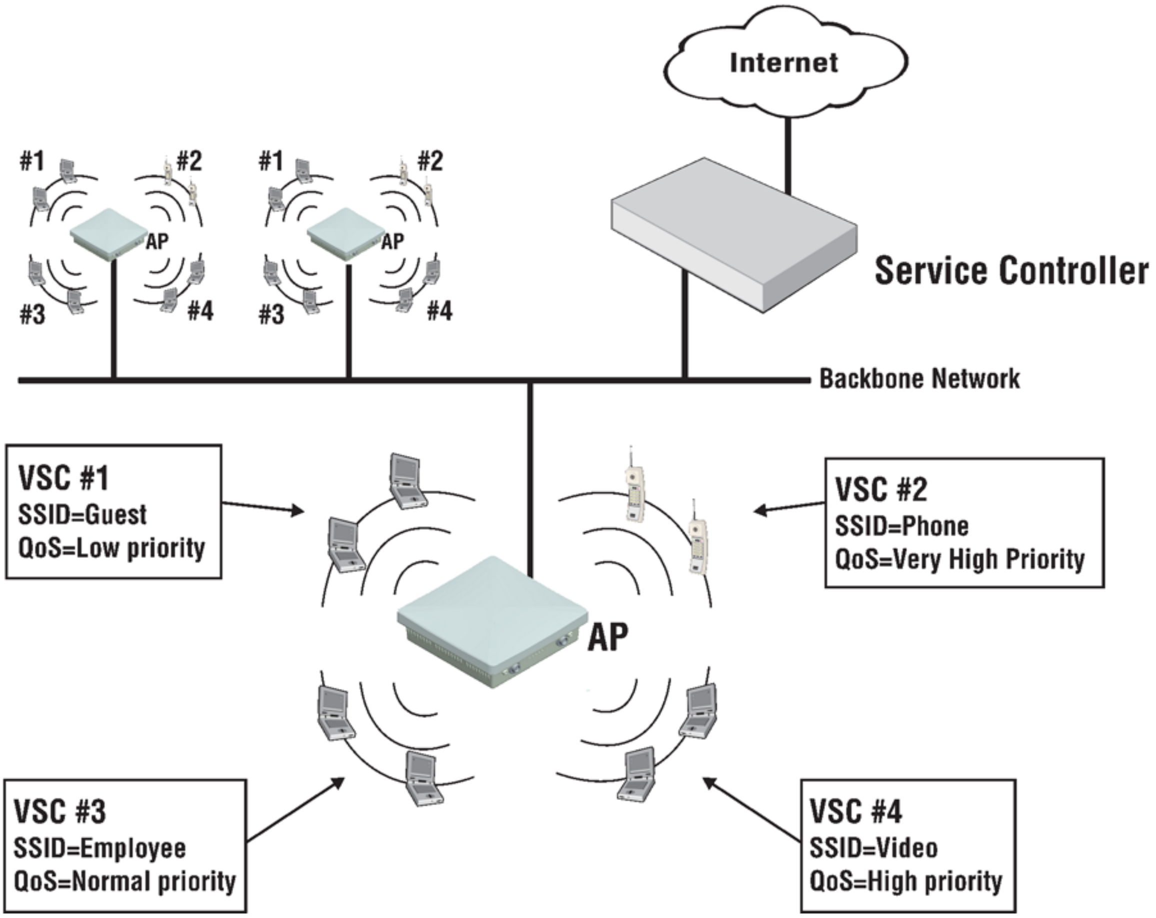


Figure 1-5: VSCs

1.3 Product Summary

All 5000 Series models provide the same full-featured network services, enabling a single architecture to be deployed across a range of locations.

Wi² series products						
Feature	Wi²-CTRL-10		Wi²-CTRL-40		Wi²-CTRL-200	
	Access Service	Mobility Pack	Access Service	Mobility Pack	Access Service	Mobility Pack
Fast roaming		X		X		X
VoWLAN support	X	X	X	X	X	X
MAP management	X	X	X	X	X	X
Public Access Interface	X	X	X	X	X	X
Maximum APs in controlled mode	10		40		200	
Maximum Public users	100		500		2000	
Network interfaces (2)	10/100/1000 Ethernet		10/100 Ethernet		10/100/1000 Ethernet	

1.4 New in this Release

New feature or enhancement	For more information see
Provisioning of controlled APs	"Provisioning" on page 75.
Embedded RADIUS server	"Using the Integrated RADIUS Server" on page 212.
Local termination of 802.1X users	
Local termination of MAC users	
Active Directory integration	"Using an Active Directory Server" on page 222
Enhanced local-user accounts	"Locally-defined User Accounts" on page 266.
Subscription plans	"Defining Subscription Plans" on page 273.
Local mesh in controlled mode	"Local Mesh" on page 291.
Enhanced autonomous AP support	"Working with Autonomous APs" on page 325.

1.5 Product Registration

To register your product, go to www.alvarion.com. On the home page select **Support** > **Product Registration** and follow the directions.

2

Chapter 2 - Controller Hardware

In This Chapter:

2.1 Introduction

The MultiService Controller family from Alvarion Networks provide similar features sets and differ only in capacity and physical appearance. This chapter describes important MultiService Controller hardware features including network ports and status lights.

Before permanently installing devices, it is recommended that you first familiarize yourself with the product by working with it as described in “Getting Started” on page 25.

⚠ **CAUTION**

Shielded Ethernet cables must be used for all connections.

2.2 Wi^2-CTRL-10

CAUTION

If the Wi²-CTRL-10 will be powered via Power over Ethernet (PoE 802.3af) ensure that only a Gigabit-compatible power injector is used. PoE injectors designed for 10/100 networks only are NOT compatible with the Wi²-CTRL-10.

The Wi²-CTRL-10 front and back panels look like this:

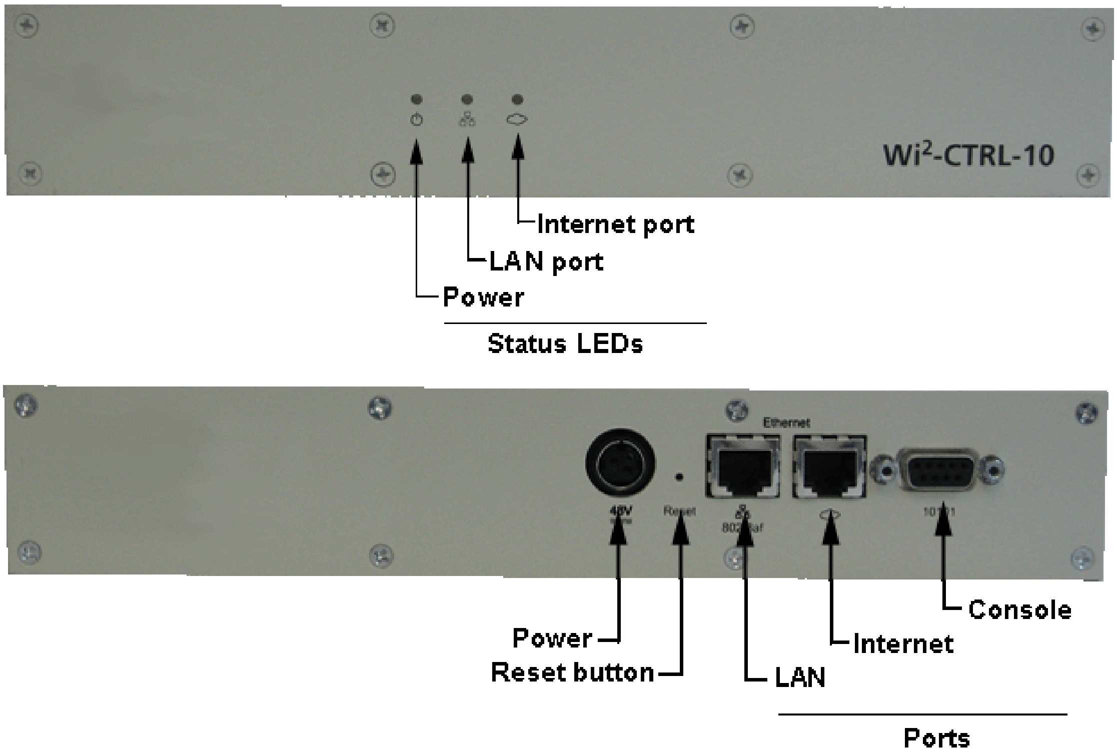


Figure 2-1: Wi²-CTRL-10 Front and Back Panels

2.2.1 Ports and Buttons

2.2.1.1 LAN Port and Internet Port

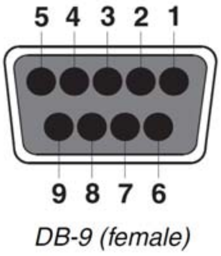
The Wi²-CTRL-10 has auto-sensing 10/100/1000 Ethernet ports, each with a corresponding status light on the front panel. The LAN port supports Power over Ethernet (PoE), enabling the Wi²-CTRL-10 to be powered by a PoE switch or PoE power injector.

2.2.1.2 Reset Button

Press and quickly release the button to restart the Wi² controler. This button can also be used to reset the Wi²-CTRL-10 to factory defaults as described in "Resetting to Factory Defaults" on page 359.

2.2.1.3 Console Port

The Wi²-CTRL-10 provides a DB-9 (female) Console (serial) port connector. The DB-9 connector (DCE) has pin assignments as follows:

Pin	Signal	Direction	Connector
1	DCD	→ to PC	 *DB-9 (female)*
2	RXD	→ to PC	
3	TXD	← from PC	
4	DTR	← from PC	
5	GND		
6	DSR	→ to PC	
7	RTS	← from PC	
8	CTS	→ to PC	
9	Unused		

To connect to a computer, use a standard (straight through) serial cable (male-to-female).

2.2.2 Status Lights

All three Wi²-CTRL-10 status lights are located on the front panel.

Light	State	Description
Power	Off	The service controller has no power.
	Flashing	The service controller is starting up. If the power light continues to flash after several minutes, it indicates that the firmware failed to load. Reset or power cycle the service controller. If this condition persists, contact Alvarion Customer Support at www.alvarion.com.
	On	The service controller is fully operational.
Ethernet: **LAN** and **Internet**	Off	Port is not connected or there is no activity.
	Flashing	Port is transmitting or receiving.
	On	Stays on for a short period when the link is established.

2.3 Wi^2-CTRL-40

The Wi²-CTRL-40 front panel looks like this:

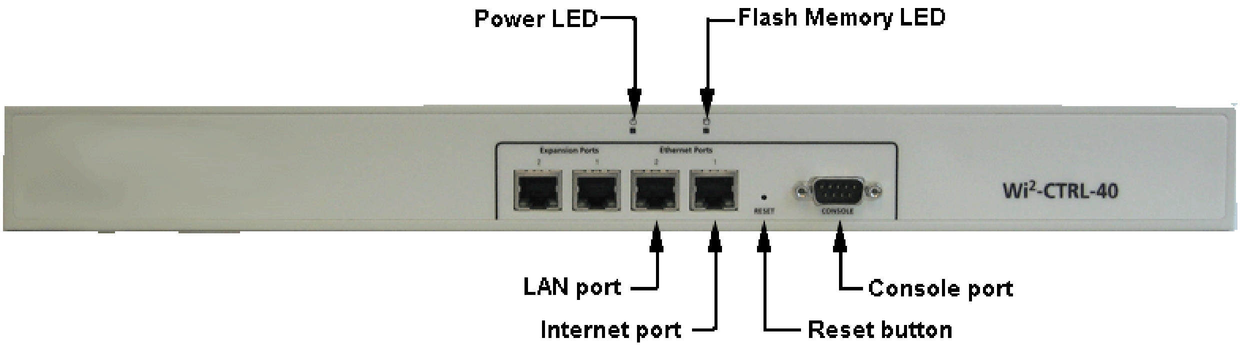


Figure 2-2: Wi²-CTRL-40 Front Panel

2.3.1 Ports and Buttons

NOTE

There are no ports on the back of the Wi²-CTRL-40.

NOTE

Expansion Ports 1 and **2** are reserved for future use.

2.3.2 LAN Port and Internet Port

Auto-sensing 10/100 Ethernet ports, each with status lights on the left and right port edges.

2.3.2.1 Reset Button

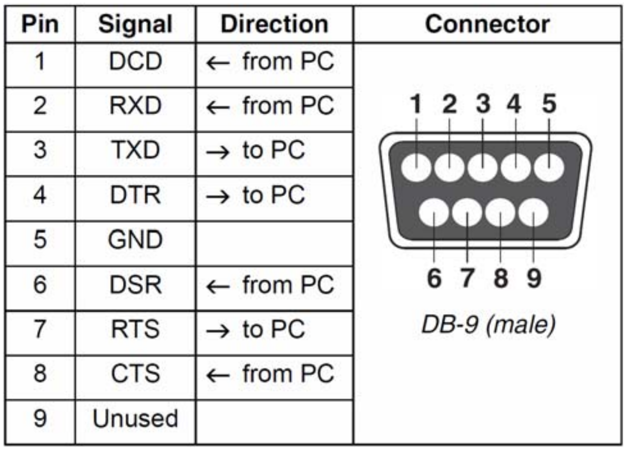
Press and quickly release the button to restart the Wi² controler. This button cannot reset the Wi²-CTRL-40 to factory defaults. For details on how to do this, see “Resetting to Factory Defaults” on page 359.

2.3.2.2 Power Switch

The Wi²-CTRL-40 power switch is located on the back next to the power cable connector. Push the switch into the **1** position for **On** or the **0** position for **Off**.

2.3.2.3 Console Port

The Wi²-CTRL-40 provides a DB-9 (male) Console (serial) port connector (DTE). The DB-9 connector has pin assignments as follows:



Pin	Signal	Direction	Connector
1	DCD	← from PC	1 2 3 4 5 6 7 8 9 *DB-9 (male)*
2	RXD	← from PC	
3	TXD	→ to PC	
4	DTR	→ to PC	
5	GND		
6	DSR	← from PC	
7	RTS	→ to PC	
8	CTS	← from PC	
9	Unused		

To connect to a computer, use the supplied null-modem serial cable.

2.3.3 Status Lights

All status lights are located on the Wi²-CTRL-40 front panel.

Light	State	Description
Power	Off	The service controller has no power. The Power switch may be in the 0 (Off) position.
	Flashing	The service controller is starting up. If the power light continues to flash after several minutes, it indicates that the firmware failed to load. Reset or power cycle the service controller. If this condition persists, contact Alvarion Customer Support at www.alvarion.com.
	On	The service controller is fully operational.
Flash memory	On (briefly)	Flash memory is being read from or written to.
LAN/Internet ports (left edge)	Off	No Ethernet link.
	Flashing	Transmit/receive activity.
	On	Ethernet link but no transmit/receive activity.
LAN/Internet ports (right edge)	Off	Link speed 10 Mbps
	On	Link speed 100 Mbps

2.3.4 Mounting Tips

Before mounting any service controller device it is recommended that you first perform its Initial Configuration as described in “Getting Started” on page 25.

2.4 Wi^{2}-CTRL-200

The Wi^{2}-CTRL-200 front and back panels look like this:

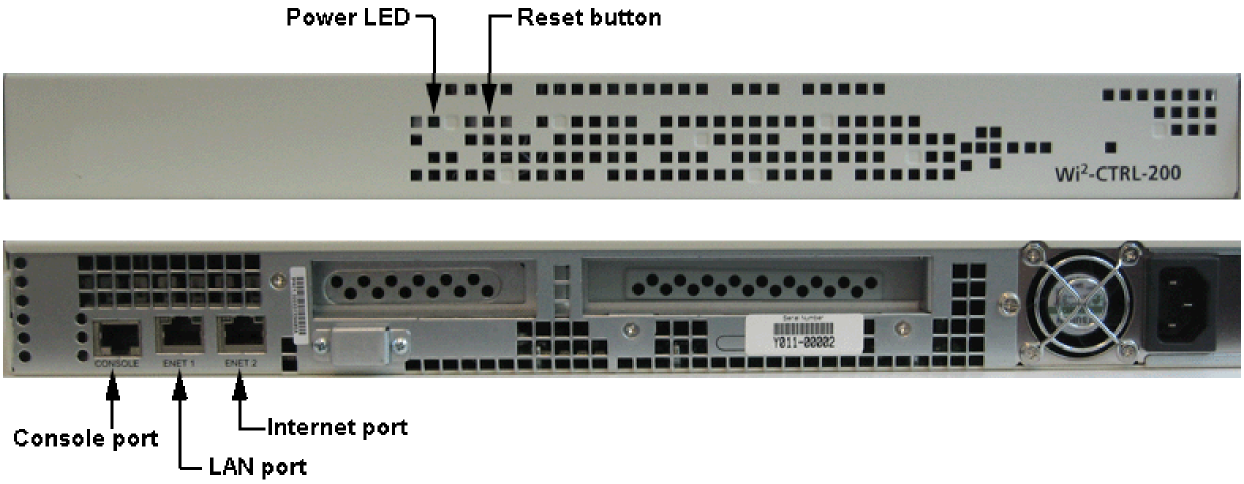


Figure 2-3: Wi^{2}-CTRL-200

NOTE

The port to the right of the Internet port is reserved for future use.

2.4.1 Ports and Buttons

2.4.1.1 LAN Port and Internet Port

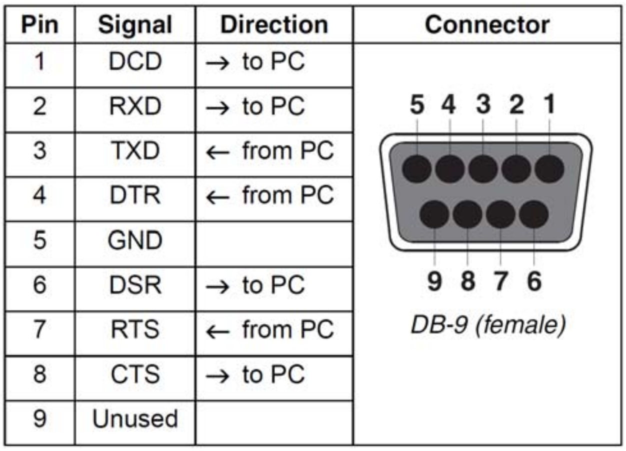
Auto-sensing 10/100/1000 Ethernet ports, each with status lights on the left and right port edges.

2.4.1.2 Reset Button

Press and quickly release the button to restart the Wi^{2} controler. This button cannot reset the Wi^{2}-CTRL-200 to factory defaults. For details on other ways to do this, see "Resetting to Factory Defaults" on page 359.

2.4.1.3 Console Port

The Wi^{2}-CTRL-200 provides an RJ-45 Console (serial) port connector. Connect the supplied RJ-45 to DB-9 (female) adapter. The DB-9 connector (DCE) has pin assignments as follows:



Pin	Signal	Direction	Connector
1	DCD	→ to PC	5 4 3 2 1 9 8 7 6 *DB-9 (female)*
2	RXD	→ to PC	
3	TXD	← from PC	
4	DTR	← from PC	
5	GND		
6	DSR	→ to PC	
7	RTS	← from PC	
8	CTS	→ to PC	
9	Unused		

To connect to a computer, use a standard (straight through) serial cable (male-to-female).

2.4.2 Status Lights

Status lights are located on both the front and back of the Wi²-CTRL-200.

Light	State	Description
Power (front)	Off	The service controller has no power.
	Flashing	The service controller is starting up. If the power light continues to flash after several minutes, it indicates that the firmware failed to load. Reset or power cycle the service controller. If this condition persists, contact Alvarion Customer Support at www.alvarion.com.
	On	The service controller is fully operational.
LAN/Internet ports (right edge)	Off	No Ethernet link.
	Flashing	Transmit/receive activity.
	On	Ethernet link but no transmit/receive activity.
LAN/Internet ports (left edge)	Off	Link speed 10 Mbps
	On (green)	Link speed 100 Mbps
	On (orange)	Link speed 1000 Mbps (gigabit)

2.4.3 Mounting Tips

Before mounting any service controller device it is recommended that you first perform its Initial Configuration as described in "Getting Started" on page 25.

3

Chapter 3 - Getting Started

In This Chapter:

3.1 Overview

This section walks you through the steps needed to configure the services controller and establish a wired connection through the service controller to the Internet.

TIP

For complete descriptions and detailed configuration instructions for a wide range of service controller applications, see the *Deployment Guide*.

A service controller is managed via its web-based management tool using at least Microsoft Internet Explorer 7.0 or Mozilla Firefox 2.0. The following diagram shows a sample setup that can be used for initial configuration and experimentation with the service controller and its features.

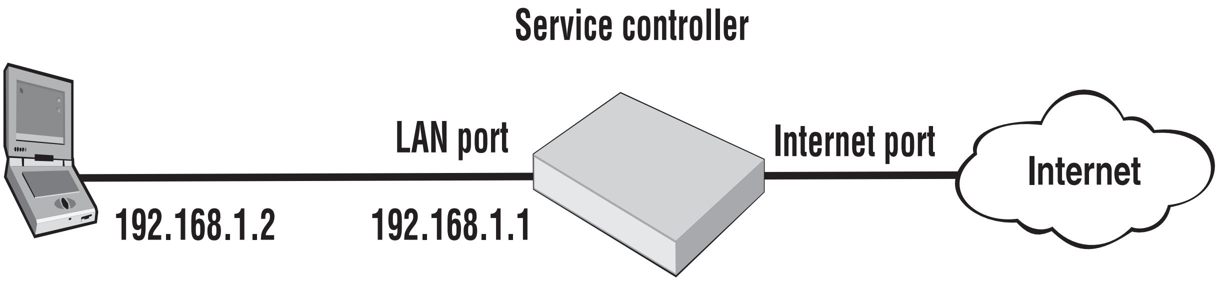


Figure 3-1: Sample Setup for Initial Configuration

3.2 Configuration Procedure

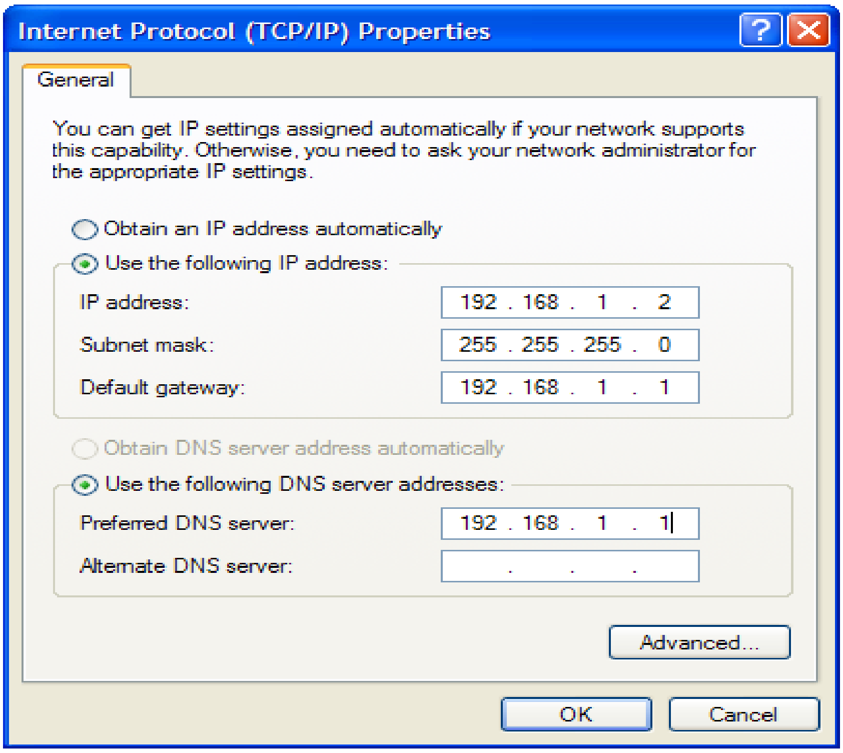
NOTE

Do not power on Alvarion Ltd. hardware until directed.

To configure the management computer

Select the computer from which you will access the service controller management tool and temporarily configure its LAN port to use a static IP address in the range 192.168.1.2 to 192.168.1.254 and a subnet mask of 255.255.255.0. Set the Default gateway and DNS server to 192.168.1.1.

For example, in Windows XP, select **Control Panel** > **Network Connections** > **Local Area Connection** > **Properties** > **Internet Protocol** > **Properties**.



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 192 . 168 . 1 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 1 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 1 . 1
Alternate DNS server: . . .

Figure 3-2: TCP/IP Properties Window

To make these connections

1. Disconnect any cable from your computer's LAN port, and disable any wireless connection.
2. Connect the service controller LAN port to your computer's LAN port.
3. Connect the service controller Internet port to a network with Internet access or to the PC port of a broadband modem or equivalent.

To start the service controller

1. Power on the service controller.
2. In a web browser, open the page: **https://192.168.1.1**.

NOTE

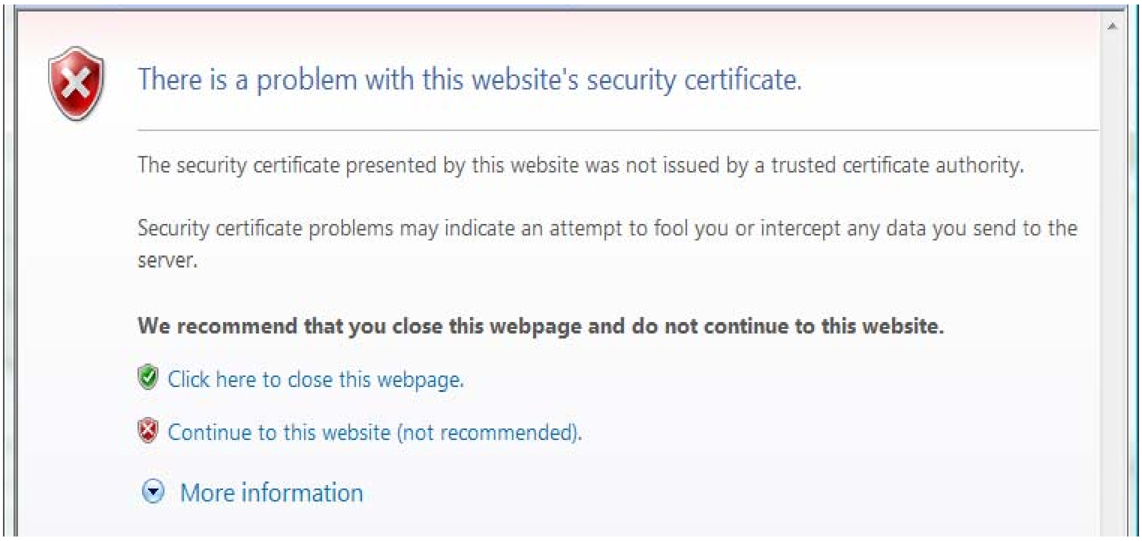
It is recommended that you use at least Microsoft Internet Explorer 7.0 or Mozilla Firefox 2.0

To perform these initial tasks after login

1. When logging in, you are prompted to accept a security certificate. To continue to work with the management tool without, proceed as follows: At the security certificate prompt, in Microsoft Internet Explorer 7, select **Continue to this website**; in Firefox 2, select **Accept this certificate temporarily for this session** and **OK**.

   For information on how you can replace the Secure Sockets Layer (SSL) certificate that ships with the service controller with one of your own, see "Managing Certificates" on page 248.

   The following is an example of a security warning displayed by Internet Explorer 7.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

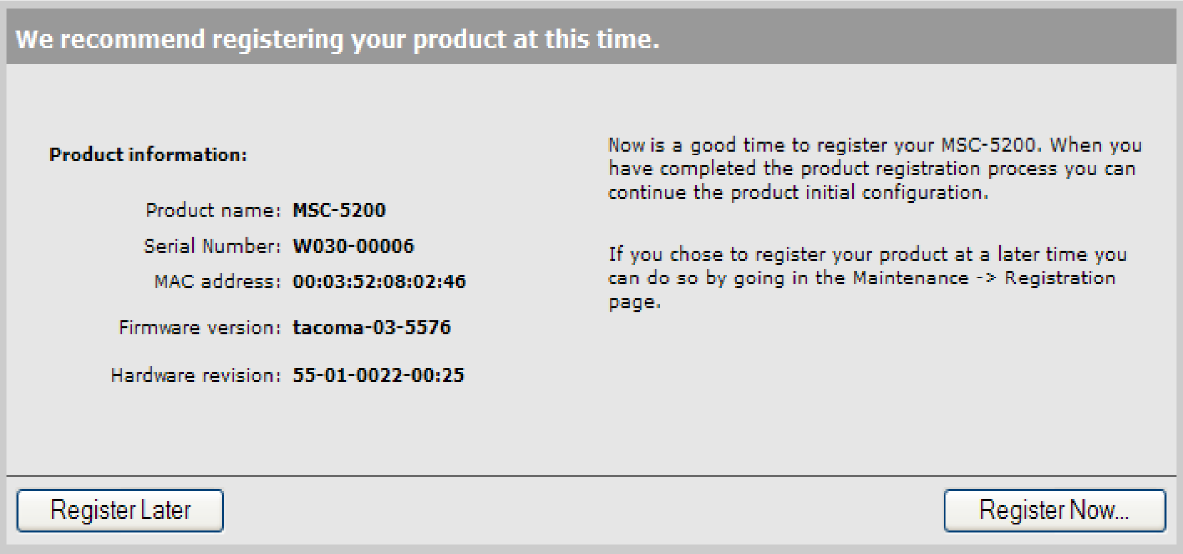
Click here to close this webpage.
Continue to this website (not recommended).
More information

Figure 3-3: Windows Security Warning

2 On the Login page, specify **admin** for **Username** and **Password** and then select **Login**.

3 On the License Agreement page, read and then select **Accept License Agreement**.

4 On the registration page it is recommended that you select **Register Now** and register the service controller. A working Internet connection is needed on the Internet port for this to work. You you can register later by selecting **Maintenance** > **Registration**.



We recommend registering your product at this time.

Product information:

Product name:	MSC-5200
Serial Number:	W030-00006
MAC address:	00:03:52:08:02:46
Firmware version:	tacoma-03-5576
Hardware revision:	55-01-0022-00:25

Now is a good time to register your MSC-5200. When you have completed the product registration process you can continue the product initial configuration.

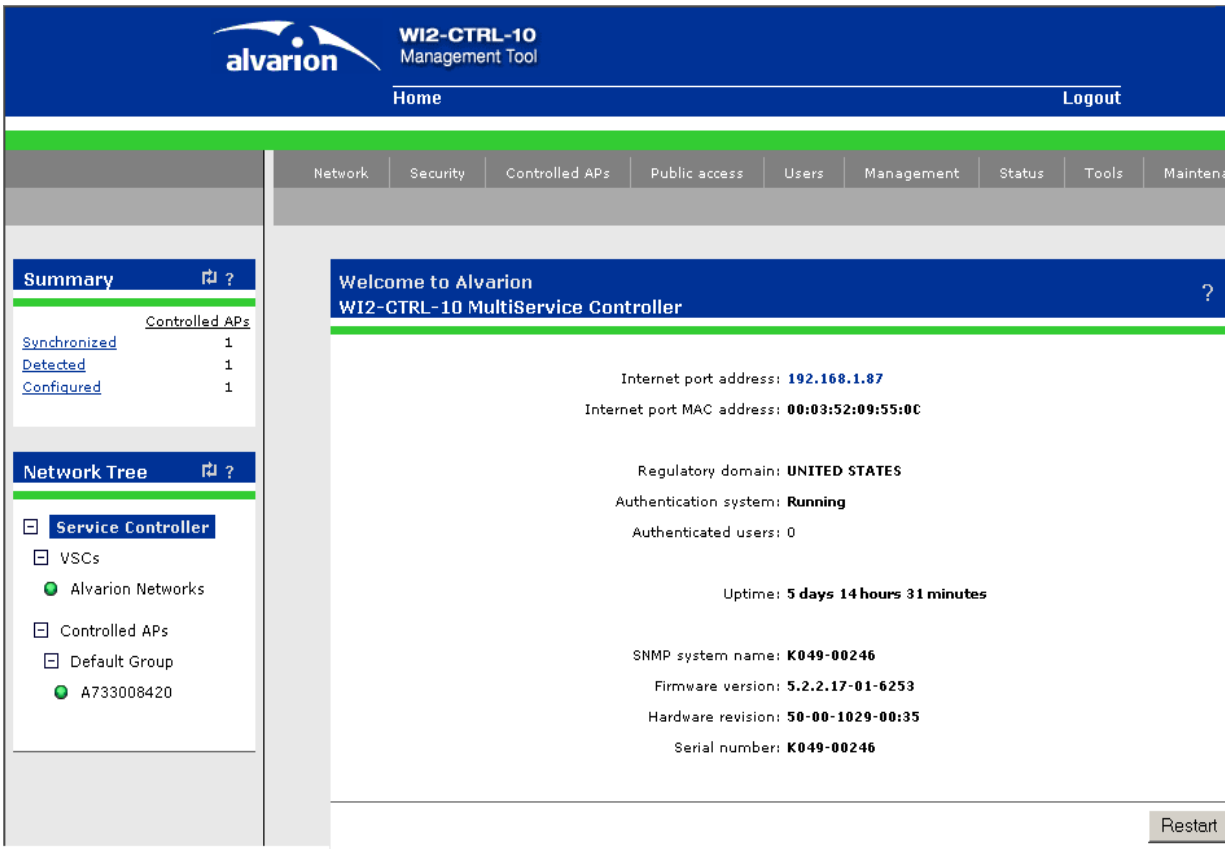
If you chose to register your product at a later time you can do so by going in the Maintenance -> Registration page.

Figure 3-4: Registration Window

5 At the **Country** prompt, select the country in which this product will be used and select **Save**.

6 At the password prompt it is recommended that you change the password. Specify the new password and select **Save**.

The management tool home page opens.



Summary

	Controlled APs
Synchronized	1
Detected	1
Configured	1

Network Tree

- Service Controller
  - VSCs
    - Alvarion Networks
  - Controlled APs
    - Default Group
      - A733008420

Welcome to Alvarion
WI2-CTRL-10 MultiService Controller

Internet port address: 192.168.1.87
Internet port MAC address: 00:03:52:09:55:0C

Regulatory domain: UNITED STATES
Authentication system: Running
Authenticated users: 0

Uptime: 5 days 14 hours 31 minutes

SNMP system name: K049-00246
Firmware version: 5.2.2.17-01-6253
Hardware revision: 50-00-1029-00:35
Serial number: K049-00246

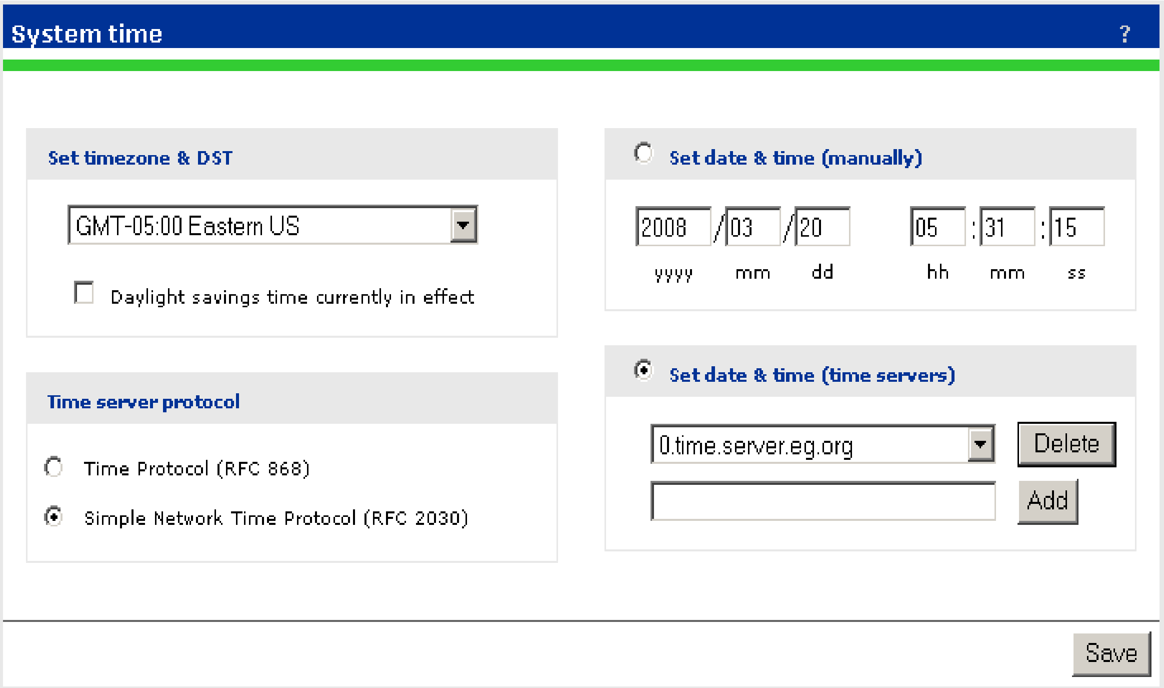
Figure 3-5: Management Tool Home Page

To configure the time server

NOTE

If you do not yet have an Internet connection on the service controller Internet port, you can temporarily set the time manually with the **Set date & time (manually)** option. **However, It is important to configure a reliable time server on the service controller**. Correct time is particularly important when the service controller is managing controlled APs, when installing certificates, and for troubleshooting. The time configured on the service controller is used on all controlled APs. Synchronization and certificate problems can occur if the service controller time is not accurate.

1 In the management tool, select **Service Controller** >> **Management** > **System time**.



System time

Set timezone & DST

GMT-05:00 Eastern US

□ Daylight savings time currently in effect

Time server protocol

○ Time Protocol (RFC 868)

● Simple Network Time Protocol (RFC 2030)

○ Set date & time (manually)

2008 / 03 / 20 — 05 : 31 : 15

yyyy mm dd — hh mm ss

● Set date & time (time servers)

0.time.server.eg.org

Figure 3-6: Configuring System Time

2 Set **timezone & DST** as appropriate.

3 Set **Time server protocol**, to **Simple Network Time Protocol**.

4 Select **Save** and verify that the date and time is updated accurately. (A working Internet connection on the service controller Internet port is required.)

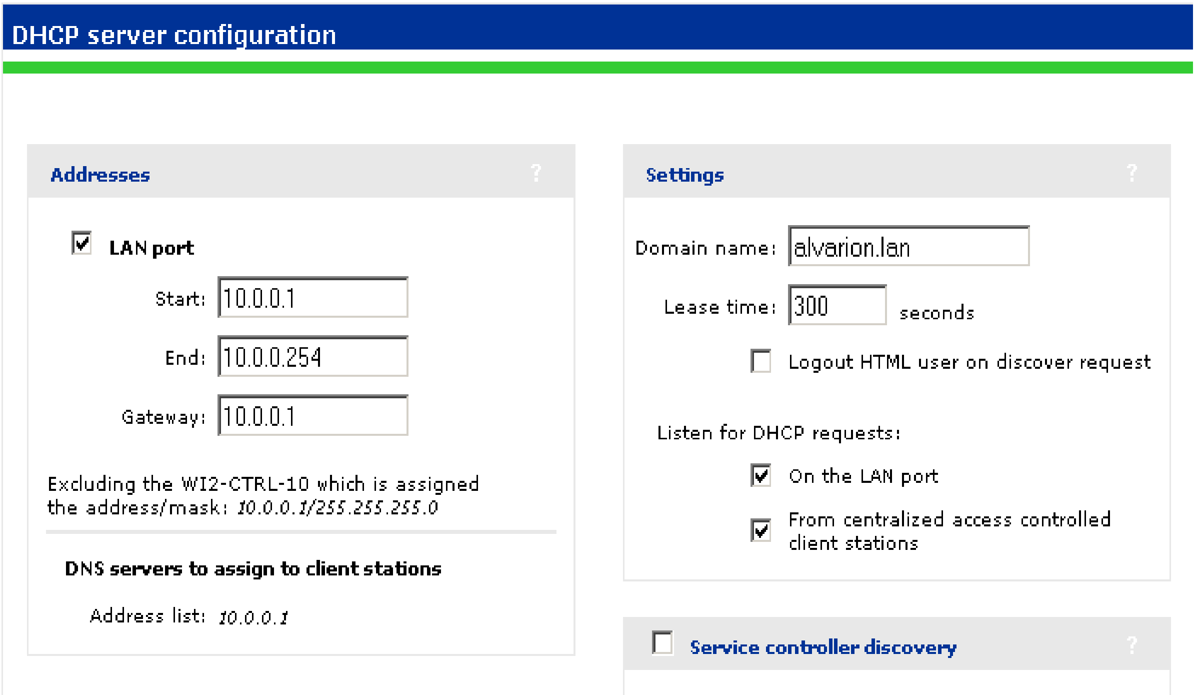
To optionally enable the DHCP server

CAUTION

DO NOT enable the DHCP server if the network to which the LAN port will be connected has its own DHCP server.

The DHCP server is useful for automatically assigning IP addresses to devices such as APs and their wireless users. Enable the DHCP server as follows:

1 Select **Service Controller** >> **Network** > **Address allocation**, select **DHCP server**, and then **Configure**.



DHCP server configuration

Addresses

☑ LAN port

Start: 10.0.0.1

End: 10.0.0.254

Gateway: 10.0.0.1

Excluding the WI2-CTRL-10 which is assigned the address/mask: *10.0.0.1/255.255.255.0*

DNS servers to assign to client stations

Address list: *10.0.0.1*

Settings

Domain name: alvarion.lan

Lease time: 300 seconds

☐ Logout HTML user on discover request

Listen for DHCP requests:

☑ On the LAN port

☑ From centralized access controlled client stations

☐ Service controller discovery

Figure 3-7: Enabling DHCP Server

2 Define the **Start** and **End** addresses. The Gateway is automatically assigned, based on the IP address and and mask configured on the LAN Port.

3 and set the **Gateway** to the IP address of the service controller.

4 Select **Save**.

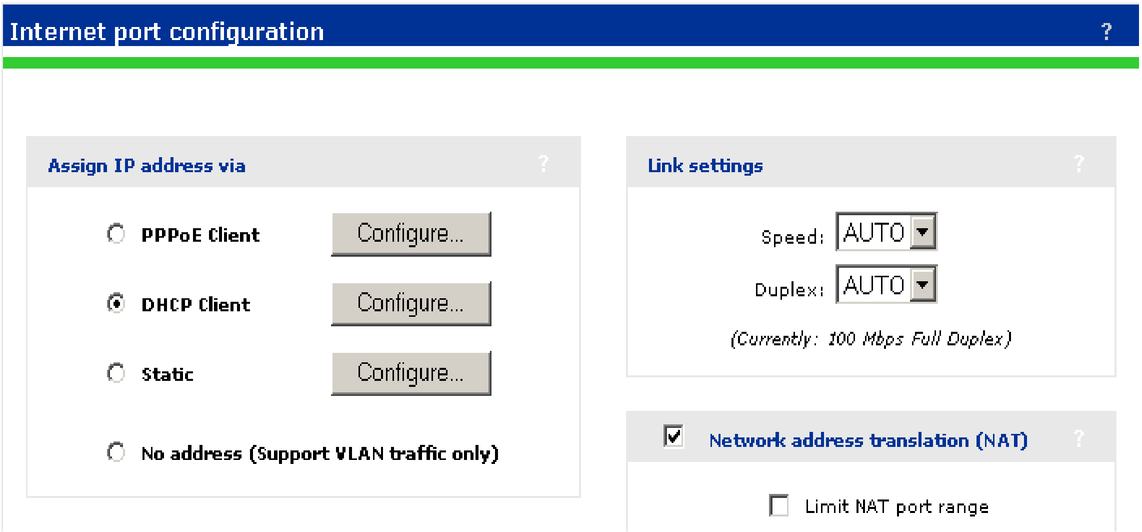
To configure the Internet port

The Internet port defaults to being a DHCP client. To verify and possibly adjust Internet port configuration, follow this procedure:

NOTE

If your Internet service provider or network administrator requires a different configuration, for example a static IP address assignment, refer to “Internet Port Configuration” on page 154.

1 Select **Service Controller** >> **Network** > **Ports** > **Internet port**. By default, **Assign IP address via** is set to **DHCP Client**. Select **Configure** next to **DHCP Client**.



Internet port configuration ?

Assign IP address via ?

○ PPPoE Client [Configure...]

● DHCP Client [Configure...]

○ Static [Configure...]

○ No address (Support VLAN traffic only)

Link settings ?

Speed: AUTO

Duplex: AUTO

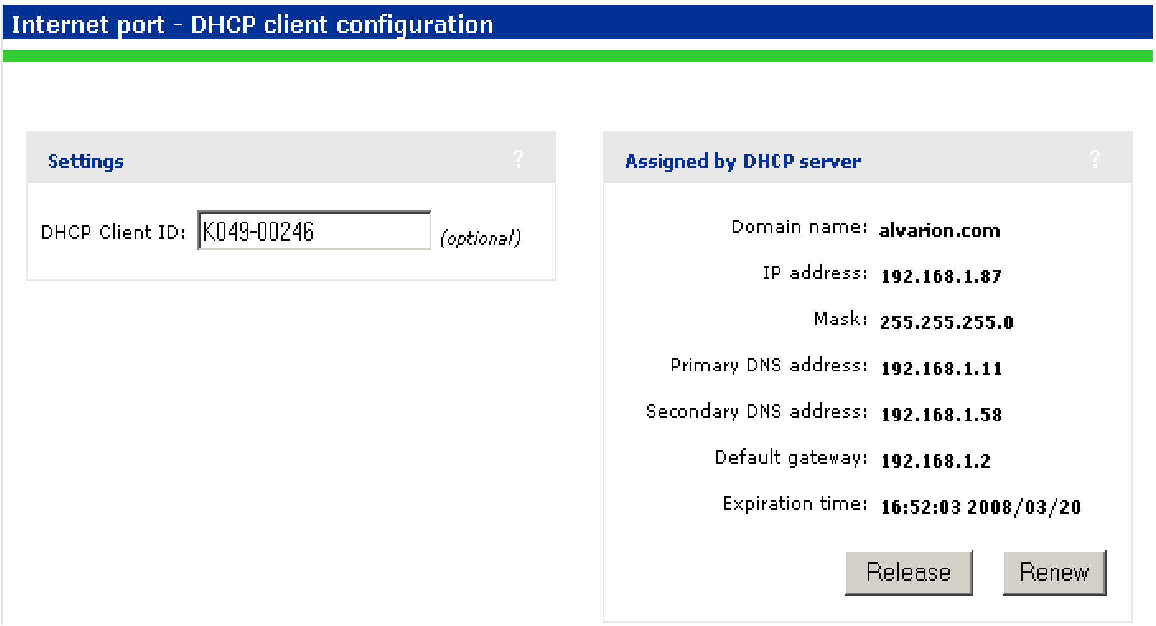
(Currently: 100 Mbps Full Duplex)

☑ Network address translation (NAT) ?

□ Limit NAT port range

Figure 3-8: Configuring the Internet Port

2 Under **Assigned by DHCP server** verify that an **IP address** is assigned.



Internet port - DHCP client configuration

Settings ?

DHCP Client ID: K049-00246 *(optional)*

Assigned by DHCP server ?

Domain name: alvarion.com

IP address: 192.168.1.87

Mask: 255.255.255.0

Primary DNS address: 192.168.1.11

Secondary DNS address: 192.168.1.58

Default gateway: 192.168.1.2

Expiration time: 16:52:03 2008/03/20

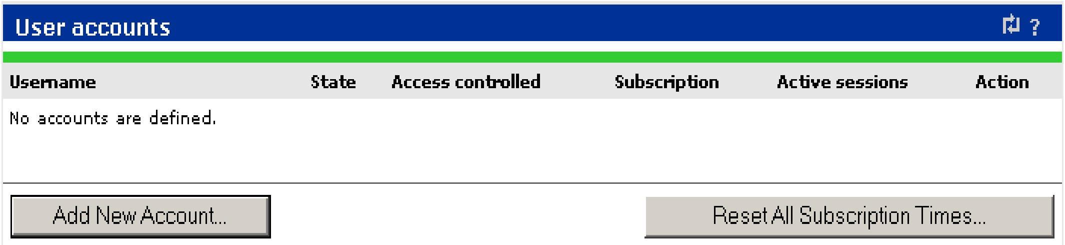
[Release] [Renew]

Figure 3-9: Verifying DHCP

To create an access-controlled account

Create an access-controlled user account for testing the public access interface as follows:

1 Select **Service Controller** >> **Users** > **User accounts** and select **Add New Account**.

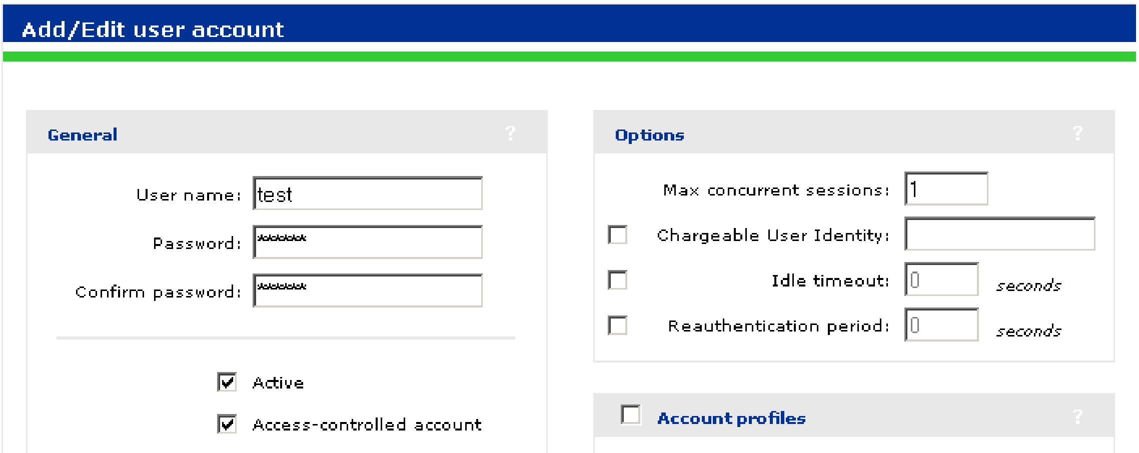


User accounts

Username	State	Access controlled	Subscription	Active sessions	Action
No accounts are defined.					

Figure 3-10: Creating an Access-Controlled Account

2 On the **Add/Edit user account**, under **General**, specify a **User name** and **Password** for the account (**test** for example) and select **Save**.



Add/Edit user account

General

User name: test

Password: ******

Confirm password: ******

☑ Active

☑ Access-controlled account

Options

Max concurrent sessions: 1

□ Chargeable User Identity:

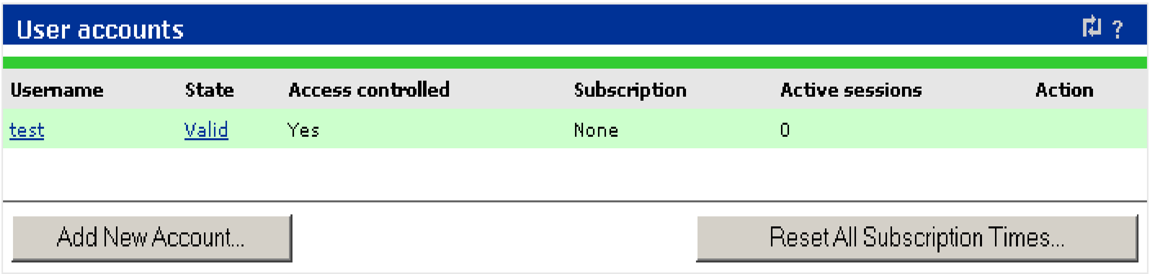
□ Idle timeout: 0 seconds

□ Reauthentication period: 0 seconds

□ Account profiles

Figure 3-11: Specifying User Name and Password

3 Confirm that the **User accounts** list shows the new account. The update will take a few seconds.



User accounts

Username	State	Access controlled	Subscription	Active sessions	Action
test	Valid	Yes	None	0	

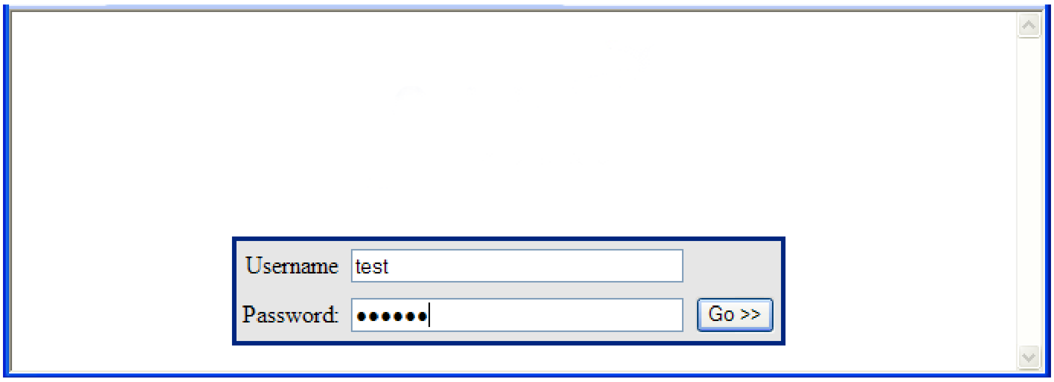
Figure 3-12: Verifying Account Creation

To test the public access interface

NOTE

This step does not require an AP for connection. Your existing wired connection to the service controller LAN port is used to test the public access interface. The Internet port must be connected to the Internet.

1 In a web browser specify the address of an Internet site such as **www.alvarion.com**. The service controller intercepts the URL and opens the public access interface Login page. Specify the **Username** and **Password** for the test account you created earlier.


Username: test

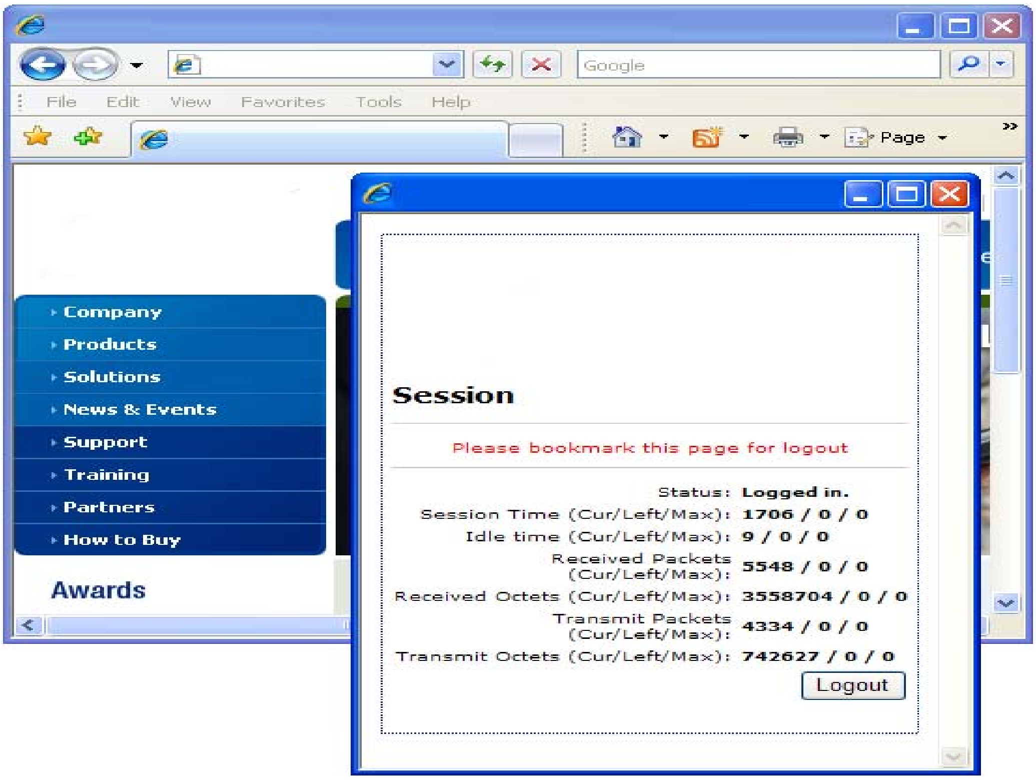
Password: ••••••

Figure 3-13: Login Window

2 Both the desired web page and the public access interface session page open.

NOTE

A popup blocker will prevent display of the Session page.



Session

Please bookmark this page for logout

Status: Logged in.
Session Time (Cur/Left/Max): 1706 / 0 / 0
Idle time (Cur/Left/Max): 9 / 0 / 0
Received Packets (Cur/Left/Max): 5548 / 0 / 0
Received Octets (Cur/Left/Max): 3558704 / 0 / 0
Transmit Packets (Cur/Left/Max): 4334 / 0 / 0
Transmit Octets (Cur/Left/Max): 742627 / 0 / 0

Logout

Figure 3-14: Public Access Interface Page

3 When finished, close the web browser.

4

Chapter 4 - Working with Controlled APs

In This Chapter:

4.1 Key Concepts

The service controller provides centralized management of APs operating in controlled mode. Controlled mode greatly simplifies the set up and maintenance of a Wi-Fi infrastructure by centralizing the configuration and management of distributed APs.

NOTE

Starting with AOS 5.x, APs operate in controlled mode by default. If you upgrade an AP from an earlier release, the AP boots in autonomous mode. Subsequently resetting the AP to factory defaults switches it to controlled mode. For details on working with autonomous APs, see “Working with Autonomous APs” on page 325. See also, “Resetting to Factory Defaults” on page 359.

4.1.1 Plug and Play Installation

In most cases, initial configuration of an AP is not required. Simply power it up and plug it into a network that provides access to a service controller. The AP will automatically discover and authenticate itself with the service controller. The AP does not offer wireless services until it successfully connects with a service controller. (Layer 3 networks may require the APs to be provisioned first.)

4.1.2 Automatic Firmware Updates

Once an AP is establishes a control channel with a service controller its firmware is automatically updated to match the version installed on the service controller.

4.1.3 Centralized Configuration Management

All AP configuration settings are defined using the service controller’s management tool and are automatically uploaded to all controlled APs with a single mouse click. For added flexibility, APs can be assigned to groups, enabling each group to have customized configuration settings. If needed, the individual settings for each AP in a group can also be customized.

4.1.4 Manual Provisioning

By default, APs operating in controlled mode will automatically discover and connect with a service controller on most network topologies. However, in certain cases it may be necessary to manually configure (provision) connectivity and discovery options. Manual provisioning can be done directly on the AP, or via the service controller. When using the service controller, provisioning can be applied to entire groups making it easy to customize many APs at once.

4.1.5 Secure Control Channel

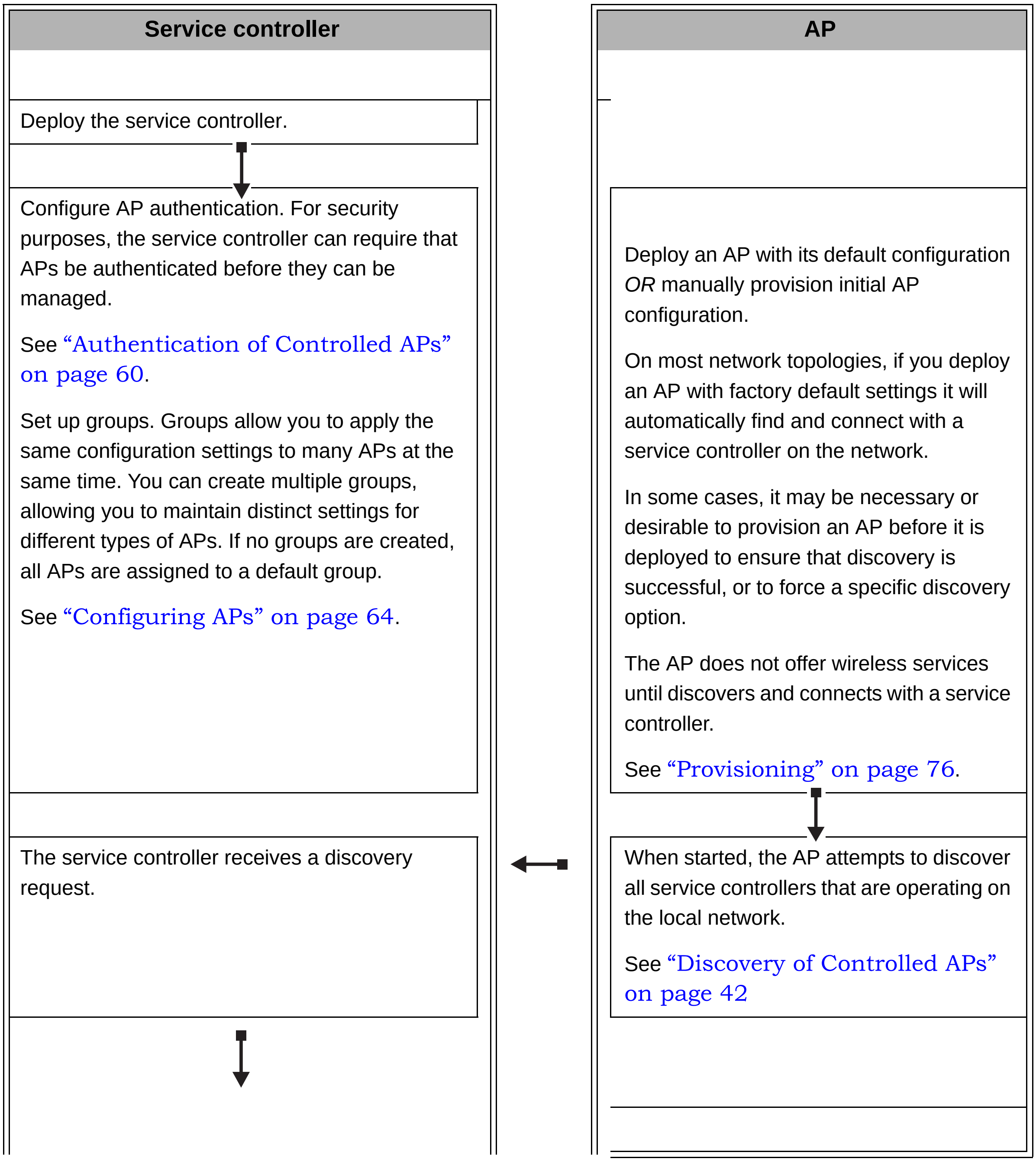
Once authenticated, a secure control channel is established between the AP and the service controller to support the exchange of management traffic between the two devices.

4.1.6 AP Authentication

The service controller can be configured to authenticate APs by their MAC address before they are managed. The authentication can be defined locally on the service controller, via a third-party RADIUS server, or using a remote text-based control file.

4.2 Key Controlled-mode Events

The following diagram provides an overview of key events that occur when working with APs in controlled mode.



Service controller

Deploy the service controller.

Configure AP authentication. For security purposes, the service controller can require that APs be authenticated before they can be managed.

See “Authentication of Controlled APs” on page 60.

Set up groups. Groups allow you to apply the same configuration settings to many APs at the same time. You can create multiple groups, allowing you to maintain distinct settings for different types of APs. If no groups are created, all APs are assigned to a default group.

See “Configuring APs” on page 64.

The service controller receives a discovery request.

AP

Deploy an AP with its default configuration *OR* manually provision initial AP configuration.

On most network topologies, if you deploy an AP with factory default settings it will automatically find and connect with a service controller on the network.

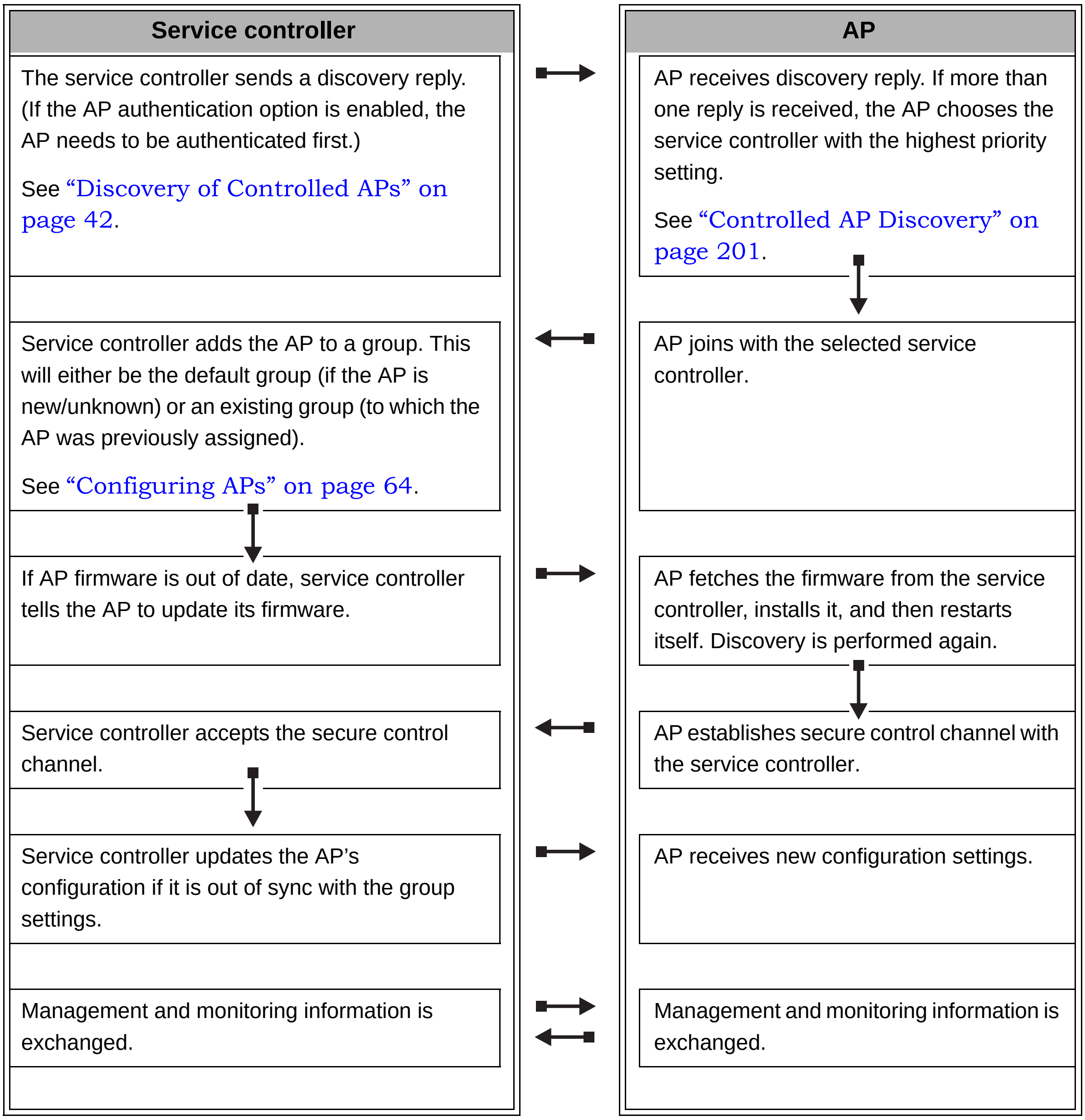
In some cases, it may be necessary or desirable to provision an AP before it is deployed to ensure that discovery is successful, or to force a specific discovery option.

The AP does not offer wireless services until discovers and connects with a service controller.

See “Provisioning” on page 76.

When started, the AP attempts to discover all service controllers that are operating on the local network.

See “Discovery of Controlled APs” on page 42



Service controller

The service controller sends a discovery reply. (If the AP authentication option is enabled, the AP needs to be authenticated first.)

See “Discovery of Controlled APs” on page 42.

Service controller adds the AP to a group. This will either be the default group (if the AP is new/unknown) or an existing group (to which the AP was previously assigned).

See “Configuring APs” on page 64.

If AP firmware is out of date, service controller tells the AP to update its firmware.

Service controller accepts the secure control channel.

Service controller updates the AP’s configuration if it is out of sync with the group settings.

Management and monitoring information is exchanged.

AP

AP receives discovery reply. If more than one reply is received, the AP chooses the service controller with the highest priority setting.

See “Controlled AP Discovery” on page 201.

AP joins with the selected service controller.

AP fetches the firmware from the service controller, installs it, and then restarts itself. Discovery is performed again.

AP establishes secure control channel with the service controller.

AP receives new configuration settings.

Management and monitoring information is exchanged.

4.3 Discovery of Controlled APs

This section describes how the discovery process works and how it can be customized.

Discovery is the process by which a controlled AP finds a service controller on a network and establishes secure control channel with it.

In most cases, the factory default configuration of an AP will result in automatic discovery of a service controller with no configuration required. However, for some network topologies it may be necessary to configure the discovery process as described in this section.

Refer to “Discovery Recommendations” on page 45 for examples of topologies that can use automatic discovery and those that require discovery to be configured.

NOTE

If you intend to manage controlled APs via local mesh, refer to “Local Mesh” on page 291.

NOTE

If you intend to manage controlled APs via local mesh, refer to “Local Mesh” on page 291.

4.3.1 Discovery Overview

Although the specifics of the discovery process vary depending on whether an AP is *unprovisioned* (in its factory default state) or *provisioned* (had its connectivity or discovery settings changed from their factory default settings), the discovery process can be summarized as follows:

1. The AP uses various methods to locate one or more service controllers that are reachable on the network. The front panel lights (“AP Status Lights” on page 49) on the AP provide a visual indication of the discovery process.
2. Discovered service controllers send a discovery reply to the AP. If the service controller is configured to require AP authentication, the reply is only sent after the AP is authenticated by the service controller.
3. The service controller adds the AP to a group. This will either be the default group (if the AP is new/unknown) or an existing group (to which the AP was previously assigned). Refer to “Wi^2 AP” on page 51 for more information.

4 The AP is now managed by the service controller, and it can be configured and monitored using the service controller’s management tool.

NOTE

APs must be connected via Port 1 to be discovered via the wired network.

NOTE

To see how this process fits into overall controlled mode operations, refer to “Key Controlled-mode Events” on page 40.

NOTE

Unprovisioned APs must obtain an IP address from a DHCP server before discovery can be initiated. When discovery occurs on a VLAN the DHCP server must be active on the VLAN.

Discovery is performed whenever an AP:

- is restarted (or reset to factory defaults),
- loses connectivity with its service controller,
- is removed and rediscovered using an action on the **Controlled APs** >> **Overview** > **Discovered APs** page.

4.3.2 Discovery Methods

Four discovery methods are available. The following table summaries their features and recommended applications.

Method	Description	Supported by	Suggested use
UDP broadcast	AP issues UDP broadcasts to discover service controllers on the same subnet.	Unprovisioned APs	Both the service controller and AP reside on the same subnet.
DHCP	AP obtains service controller address from a specially configured DHCP server.	Unprovisioned APs	The AP is on a different subnet than the service controller.

Method	Description	Supported by	Suggested use
DNS	AP obtains service controller address from a DNS server using predefined host names.	Unprovisioned APs Provisioned APs	The AP is on a different subnet than the service controller.
Specific IP addresses	AP connects to a specific service controller using a pre-configured static IP address.	Provisioned APs	DHCP and DNS are not used and the AP is on a different subnet than the service controller.

NOTE

A service controller listens for discovery requests on its LAN port and/or Internet port as configured on the **Controller >> Management > Device Discovery** page. (See "Device Discovery" on page 200).

4.3.2.1 UDP Broadcast Discovery

The AP sends a UDP broadcast to discover all service controllers that are on the same subnet as the AP.

4.3.2.2 DHCP Discovery

When configured as DHCP client (which is the factory default setting for all APs), an AP can obtain the IP addresses of service controllers on the network from any DHCP server configured to support the Alvarion Ltd. Vendor Class (DHCP option 43).

Vendor Class enables an administrator to define a list of up to three available service controllers on the network to which APs can connect.

- If the service controller is configured to operate as the DHCP server for the network, you can define the list of available service controllers by selecting **Service Controller** >> **Network** > **Address allocation** > **DHCP server** and then configure the **Service controller discovery** option.

- If an external DHCP server is used, it must have **Option 43** configured. For examples on how to configure some popular third-party DHCP servers, see DHCP Servers and Alvarion Vendor Classes.

4.3.2.3 DNS Discovery

DNS discovery is attempted using UDP unicast discovery requests which are issued by the AP to the following default service controller names:

- cnsrv1
- cnsrv2
- cnsrv3

This method enables discovery across various network configurations. It requires that at least one service controller name is resolvable via a DNS server.

The AP appends the default domain name returned by a DHCP server (when it assigns an IP address to the AP) to the service controller name. For example, if the DHCP server returns **mydomain.com**, then the AP will search for the following service controllers in this order:

- cnsrv1.mydomain.com
- cnsrv2.mydomain.com
- cnsrv3.mydomain.com

4.3.2.4 Discovery Using Specific IP Addresses

Provisioned APs can be configured to connect with a service controller at a specific IP address. A list of addresses can be defined, allowing the AP to search for multiple service controllers.

This can also be used to strengthen the security on a local network to make sure that the AP goes to a specific service controller for management.

4.3.3 Discovery Recommendations

- **If the AP is on the same subnet as the** service controller**,** then UDP discovery will work with no configuration required on either the AP or service controller. This applies whether the service controller is operating as the DHCP server for the network or if a third-party DHCP server is used.

  If VLANs are being used, then UDP discovery will also work with no configuration. However, to speed up the discovery process you can provision the AP with a specific VLAN ID. This will eliminate the need for the AP to find and attempt discovery on all available VLANs.

- **If the AP is on a different subnet than the service controller,** UDP discovery will not work. Instead, DHCP or DNS discovery must be used, or direct IP address discovery must be provisioned.

  - **DHCP discovery:** If you have control of the DHCP server, enable support for the Alvarion Ltd. Vendor Class as explained in "DHCP Discovery" on page 44.

  - **DNS discovery:** If you have control of the DNS server, you can configure it to resolve the default service controller names that an AP will search for. To use custom names, you must provision discovery settings on the AP. For more information on using custom names, see "Provisioning Discovery" on page 81.

  - **Specific IP discovery:** This method needs to be used when you do not have control over the DHCP and DNS servers and no domain is registered to the service controller. For example, if the connection to the service controller is routed over the public Internet.

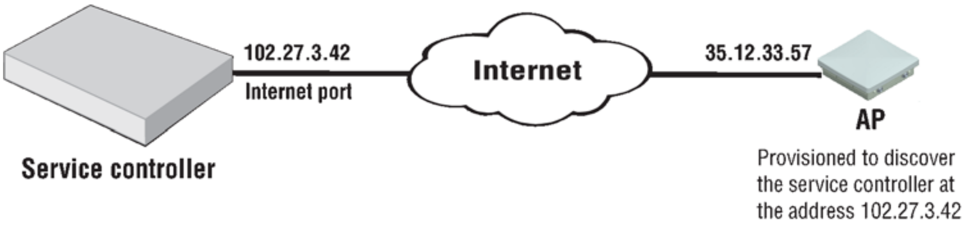

102.27.3.42
Internet port
Internet
35.12.33.57
AP
Service controller
Provisioned to discover the service controller at the address 102.27.3.42

Figure 4-1: Discovery Example

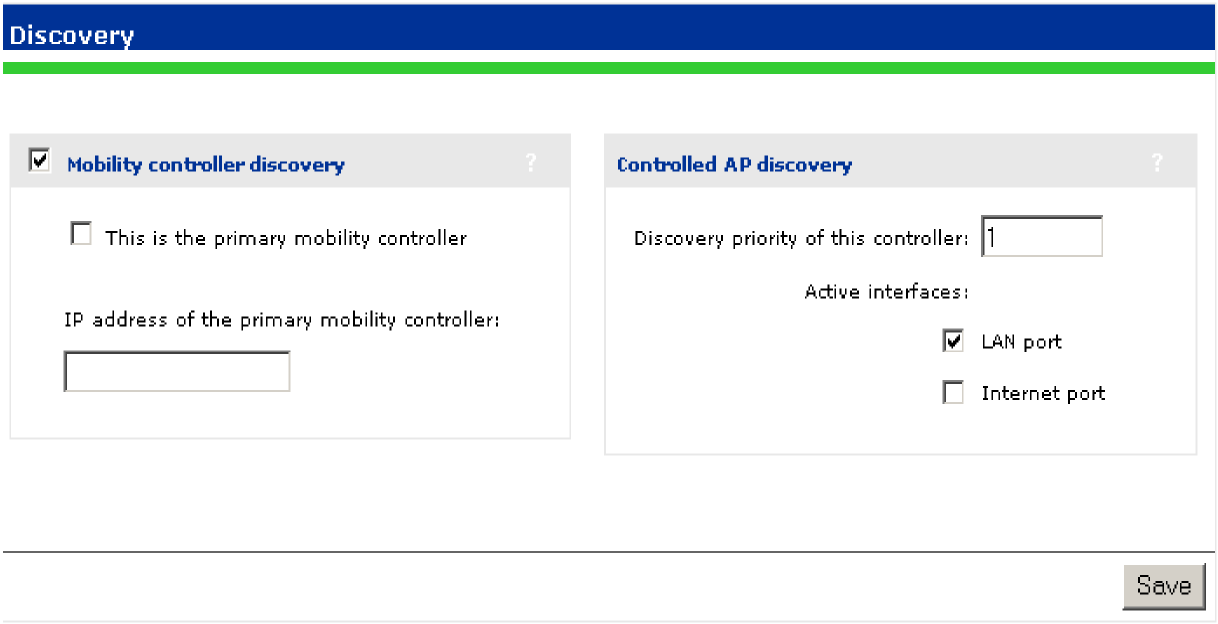
For discovery to succeed, the AP must be provisioned with the service controller's IP address. For more information, see "Provisioning Discovery" on page 81.

4.3.4 Discovery Priority

Each service controller that receives a discovery request sends the requesting AP a discovery reply. (If the AP authentication option is enabled, the AP needs to be authenticated first. Requests from unauthenticated APs are ignored.)

If an AP receives discovery replies from multiple service controllers, the AP selects the service controller that has the highest discovery priority setting.

Discovery priority is set on a service controller using the **Discovery priority of this Controller** option on the **Service Controller >> Management > Device Discovery** page.



Discovery

☑ Mobility controller discovery

☐ This is the primary mobility controller

IP address of the primary mobility controller:

Controlled AP discovery

Discovery priority of this controller: 1

Active interfaces:

☑ LAN port

☐ Internet port

Figure 4-2: Device Discovery

If two service controllers have the same high-priority setting, the AP will appear on the **Overview > Discovered APs** page of both service controllers with a **Diagnostic** value of **Priority Conflict**. To resolve the conflict, change the priority setting of one of the service controllers (**Service Controller >> Management > Device discovery** page).

4.3.5 Discovery Behavior

Discovery occurs differently for unprovisioned and provisioned APs.

4.3.5.0.1 Unprovisioned APs

Once an unprovisioned AP has received its IP address from a DHCP server (either from the service controller-based DHCP or the corporate DHCP), it attempts to discover a service controller using the following methods, in order:

- UDP broadcast
- DHCP
- DNS

These discovery methods are applied on the following interfaces, in order:

- Last interface on which a service controller was discovered. (Only applies to APs that have previously discovered a service controller)
- Untagged on Port 1.
- All other detected VLANs (in sequence) on Port 1.

4.3.5.0.2 Provisioned APs

The discovery method that is used depends on how the AP is provisioned. If discovery settings are provisioned, then the AP uses only the provisioned settings. The following discovery options are available:

- DNS discovery: Enables custom service controller names and domains to be used for discovery.
- Discovery using an IP address: Enables the AP to find service controllers operating at a specific IP address.

If only connectivity settings are provisioned, then the AP attempts to discover a service controller using the same methods as for unprovisioned APs, namely:

- UDP broadcast
- DHCP (the AP must be configured as a DHCP client for this to work)
- DNS

NOTE

For more information on provisioning APs, see “Provisioning” on page 76.

4.3.6 Discovery Considerations

The following considerations must be made with respect to discovery:

4.3.6.1 Firewall

If the network path between an AP and a service controller traverses a firewall the following ports must be opened for management and discovery to work:

Protocol	Open this port	Description
UDP	source and destination 38212 (9544 hex)	Discovery port number

UDP	1194 (4AA hex)
	source = 39064 (9898 hex)
	destination = 30840 (7878 hex)
		Secure management tunnel

TCP	source and destination 1194 (4AA hex)	Firmware updates and certificate exchanges (for the secure management tunnel)
IP	IANA port number = 47	Tunnel for centralized access control feature and the optional L3 mobility traffic feature.
UDP	destination = 1800, 1812, 1813	Location aware. This is only necessary if autonomous APs are using the access-controlled (public access) interface.

4.3.6.2 NAT

If the network path between an AP and a service controller implements NAT (network address translation), discovery will only work if NAT functions on outbound traffic sent from the AP to the service controller. If NAT operates in the other direction, discovery will fail.

4.3.7 AP Status Lights

4.3.7.1 Wi² AP

The AP status lights provide the following information during discovery:

Status light behavior	Description
Power light blinks slowly.	AP is looking for an IP address, or building the list of VLANs on which to perform discovery.
Power light, Ethernet light, and Wireless light each turn ON and OFF one after the other, moving left to right.	AP has obtained an IP address and is attempting to discover a service controller.
Power light is on. Ethernet and wireless lights blink alternately until the secure management tunnel is established.	AP has found a service controller and is attempting to establish a secure management tunnel with it.

Status light behavior	Description
Power light and Ethernet light blink alternately and quickly. Wireless light is OFF.	The AP has received a discovery reply from two or more service controllers with the same priority setting. The AP is unable to connect with either unit until the priority conflict is resolved.
Power light and Wireless light blink slowly.	AP is attempting to establish a local mesh link to a master node.
Power light and Ethernet light blink slowly.	AP is attempting to establish wired connectivity. Next pattern to look for is *Power light blinks slowly*.

Once the AP has established a secure management tunnel to a service controller the status lights function as follows:

- Power light is solid to indicate that the AP is fully operational.
- Ethernet light blinks to indicate the presence of traffic on the Ethernet port.
- Wireless light blinks to indicate the presence of traffic on the wireless port.

4.4 Wi² AP

The AP status lights provide the following information during discovery:

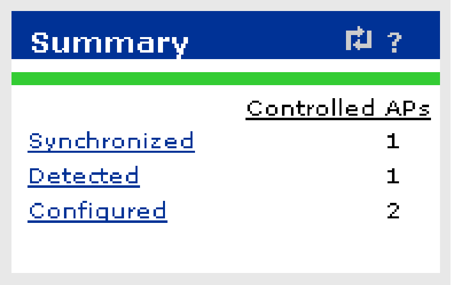
Status light behavior	Description
Power light blinks slowly.	AP is looking for an IP address, or building the list of VLANs on which to perform discovery.
Power light, Info light, and Ethernet light each turn ON and OFF one after the other, moving left to right.	AP has obtained an IP address and is attempting to discover a service controller.
Power light is on. Info and Ethernet lights blink alternately until the secure management tunnel is established.	AP has found a service controller and is attempting to establish a secure management tunnel with it.
Power light and Info light blink alternately and quickly. Ethernet light is OFF.	The AP has received a discovery reply from two or more service controllers with the same priority setting. The AP is unable to connect with either unit until the priority conflict is resolved.
Power light and one Wireless light blink slowly. (This will be the Wireless light on which the local mesh link is being established.)	AP is attempting to establish a local mesh link to a master node.
Power light and Ethernet light blink slowly.	AP is attempting to establish wired connectivity. Next pattern to look for is *Power light blinks slowly.*

Once the AP has established a secure management tunnel to a service controller the status lights function as follows:

- Power light is solid to indicate that the AP is fully operational.
- Ethernet light blinks to indicate the presence of traffic on the Ethernet port.
- Wireless light blinks to indicate the presence of traffic on the wireless port.

4.4.1 Monitoring the Discovery Process

This Summary menu lists the number of controlled APs discovered by the service controller. APs are grouped according to their management state. For example: **Synchronized**, **Detected**, **Configured**, **Pending**.



Summary

	Controlled APs
Synchronized	1
Detected	1
Configured	2

Figure 4-3: Controlled APs Summary Menu

A AP may be active in more than one state at the same time. For example, an AP may be both **Detected** and **Synchronized**. Select the state name to display information about all APs in that state.

4.4.1.1 Management States

- **Synchronized:** These APs are up and running, offer wireless services, and have had their firmware and configuration settings successfully updated by the service controller.
- **Detected:** These APs have sent a discovery request to the service controller and the service controller has replied. This does not imply that the AP received the reply from the service controller. For example, if routes are not properly configured on the service controller, the reply may be sent on the wrong interface or dropped and the AP remains in the detected state.
- **Pending:** An action is in progress. For example, firmware or configuration may be uploading to the AP or the AP is restarting.
- **Unsynchronized:** These APs are up and running and offer wireless services. However, their configuration settings do not match the settings defined on the service controller (at the group or AP level).
- **Unauthorized:** These APs have not been not authorized, either manually by an administrator or automatically by the service controller.
- **Suspicious:** These APs have unexpectedly requested new authentication certificates from the service controller. Possible causes are:
  - The AP was disconnected from the network, or turned off, for more than three days.
  - A previously synchronized AP was reset to factory defaults.

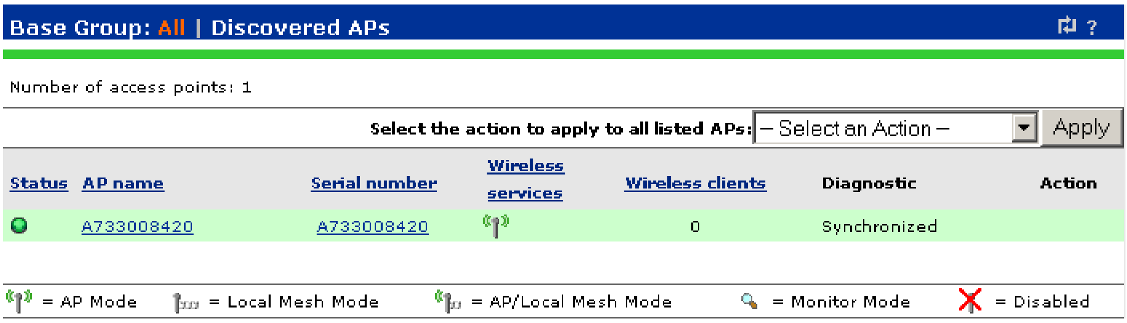
» A rogue device is trying to breach the network.

You should accept the AP as a valid device, or remove it from the network.

- **Unresponsive:** These APs that have stopped sending management information to the service controller. This is usually auto-repaired.
- **Conflicting:** These APs were created with a product type that does not match the detected product type. This can occur when APs are added manually to a group with the wrong product type. For example, an AP-320 was added as an AP-330.
- **Licensing violation:** The APs have a licensing issue that prevents them from offering all configured services. More information on which license is violated or required for the system to function can be found by selecting the AP link.

4.4.1.2 Viewing all Discovered APs

To display information about APs discovered by the service controller, select **Controlled APs** >> **Overview** > **Discovered APs**.



Base Group: All | Discovered APs

Number of access points: 1

Select the action to apply to all listed APs: – Select an Action – Apply

Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
●	A733008420	A733008420		0	Synchronized	

= AP Mode = Local Mesh Mode = AP/Local Mesh Mode = Monitor Mode ✗ = Disabled

Figure 4-4: Discovered APs List

The **Discovered APs** page provides the following information:

- **Number of access points**: Indicates the number of APs that were discovered.
- **Select the action to apply to all listed APs**: Lets you apply the selected action to all APs in the list. Select an action and then **Apply**.

  » **Status**

  - Green: The AP is synchronized, meaning that the AP is connected, running, and has received its configuration from the service controller.
  - Yellow: The AP is unsynchronized, meaning that the AP is operational but does not have the same configuration as the service controller, yet.
  - Red: The AP is not part of the controlled network and is not providing wireless services. Refer to the **Diagnostic** column for details.
  - Grey flashing: An action is pending.
  - Grey solid: The AP is configured in a group, but has not been discovered on the network.

- **AP name**: Name assigned to the AP.
- **Serial number**: Unique serial number assigned to the AP at the factory. Cannot be changed.
- **Wireless services**: Indicates the status of wireless services on the AP. A separate icon appears for each radio on the AP. Refer to the legend under the table for the meaning of each icon.
- **Wireless clients**: Indicates the number of wireless clients currently associated with the AP. Select the number to see more information.
- **Diagnostic**: Indicates the status of the AP with regards to management by the service controller, as shown in the following table.

Diagnostic	Description
Waiting for acceptance	The AP has been authorized by the service controller. However, the AP has not yet selected the service controller to function as its service controller. (If multiple service controllers replied to the APs discovery request, the AP may choose to connect with another service controller.)

Diagnostic	Description
Priority conflict	More than one service controller responded to the AP’s discovery request with the same priority. The AP is therefore unable to select a service controller to function as its service controller. The AP will retry its discovery request shortly. You must fix the priority conflict by changing the priority setting for one of the service controllers (**Service Controller >> Management > Device discovery**).
Not authorized	The AP could not be authenticated by the service controller. This may be due to invalid authentication credentials supplied by the AP. (Authentication settings used by the service controller are defined on the **Service Controller >> Security > Controlled APs** page.) You should accept the AP unless it is an actual rogue.
Not responding	The AP has stopped sending management information to the service controller. Rediscovery may re-establish the connection. If not the AP may have lost power or a network failure has occurred.
Wrong Product	The AP was created with a product type that does not match the detected product type. This can occur when an AP is manually added to a group with the wrong product type. For example, an AP-320 was added as an AP-330. You should verify and fix the product type.
Unconfigurable	This AP cannot be added because the maximum number of configured APs has been reached. To add this AP you must first remove one or more currently configured APs.
Validating Firmware	The service controller is waiting for the AP to send its firmware version number.
Uploading Firmware	The service controller is uploading new firmware to the AP. Wait until the operation completes.
Installing firmware	New firmware has been successfully uploaded to the AP. Wait until the AP restarts to activate the new firmware.
Firmware failure	New firmware failed to upload to the AP. The service controller will retry soon.
Unsupported product	No suitable firmware is available for this AP on the service controller. You should upgrade the service controller firmware so that the newly-introduced product can be recognized.

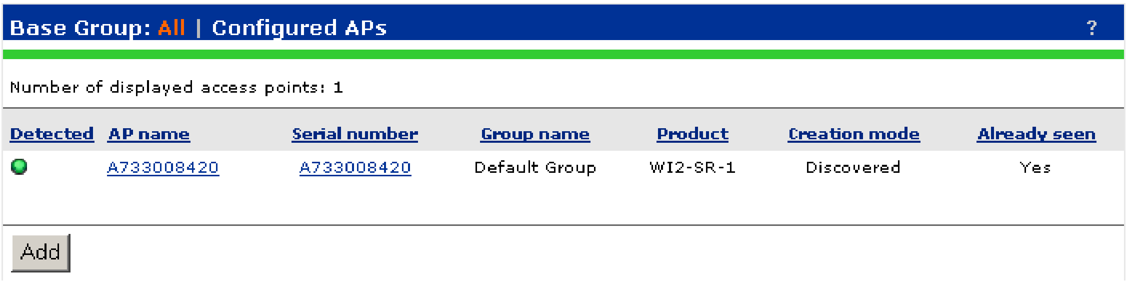
Diagnostic	Description
Establishing tunnel	A secure management connection is being established to the AP.
Suspicious device	The AP unexpectedly requested new authentication certificates from the service controller. Possible causes are as follows: - the AP was disconnected from the network, or turned off, for more than three days, - a rogue device is trying to breach the network. - a previously synchronized AP was reset to factory defaults. You should accept the AP as a valid device or remove it from the network.
Validating configuration	The service controller is waiting for the AP to send its configuration.
Uploading configuration	Configuration settings are currently being sent to the AP.
Synchronized	The AP is up and running, offers wireless services, and had its firmware and configuration settings successfully updated by the service controller.
Unsynchronized	The AP is up and running and offers wireless services. However, its configuration settings do not match the settings defined on the service controller (at the group or AP level). You should Synchronize the AP.
Resetting configuration	The AP configuration is being reset to factory defaults. This is normal and will occur when the firmware version on the service controller is changed or if the AP is not synchronized.
Validating capabilities	The capabilities of the AP are being identified by the service controller.
Invalid country	The AP cannot be configured with the current country settings defined on the service controller. This can occur when an AP manufactured for use in a specific country is deployed in another country. You should replace the AP with one configured for the same country as the service controller. Depending on the regulations, it may be possible to set the AP to the correct country.

Diagnostic	Description
Restoring configuration	The AP is currently restoring its previous configuration settings.
Rebooting	The AP is restarting.
Synchronized/License violation	Although the AP is synchronized it is non-functional (quarantined) due to a license violation. You must change the configuration to omit the affected licensed feature or acquire and install a valid license.
Unsynchronized/License violation	The AP is not synchronized but can continue operation. However, if synchronized, it will become non-functional as described above for Synchronized/License violation. Before synchronizing, either change the configuration to omit the affected licensed feature or acquire and install a valid license.
Incompatible settings	■ Local mesh has been provisioned on the AP but: ■ The APs radio is disabled. ■ The AP's radio operating mode does not support local mesh. ■ The APs radio wireless mode does not match the one provisioned. ■ The mesh ID is not uniquely assigned.
Applying radio configuration	The AP is applying its radio configuration.
Detected	The AP was detected by the service controller.

- **Action**: Indicates the recommended administrative action to be taken to resolve a diagnostic condition.

4.4.1.3 Viewing all Configured APs

To display information about APs configured by the service controller, select **Controlled APs** >> **Overview** > **Configured APs**.



Base Group: All | Configured APs ?

Number of displayed access points: 1

Detected	AP name	Serial number	Group name	Product	Creation mode	Already seen
●	A733008420	A733008420	Default Group	WI2-SR-1	Discovered	Yes

Figure 4-5: Viewing Configured APs

The **Configured APs** page provides the following information:

- **Number of displayed access points**: Number of configured APs that were discovered.
- **Detected**: Status light indicating if the AP has been detected.
  - Green: The AP has been discovery and is listed on the AP overview page, where more information is provided on the AP.
  - Red: The AP has not been discovered.
- **AP name**: Name assigned to the AP. Select the name to open its AP management page.
- **Serial number**: Serial number assigned to the AP. Select the serial number to open its AP management page.
- **Group Name**: Group that the AP is part of.
- **Product**: Product name of the AP in the Alvarion product family.
- **Creation mode**:
  - **Local**: AP was added manually, or was manually authenticated after being discovered.
  - **RADIUS**: AP was successfully authenticated via RADIUS and then created.
  - **External file**: AP was successfully authenticated using the external file option.

  - **Discovered**: Automatically detected by the service controller based on discovery-time parameter exchange.

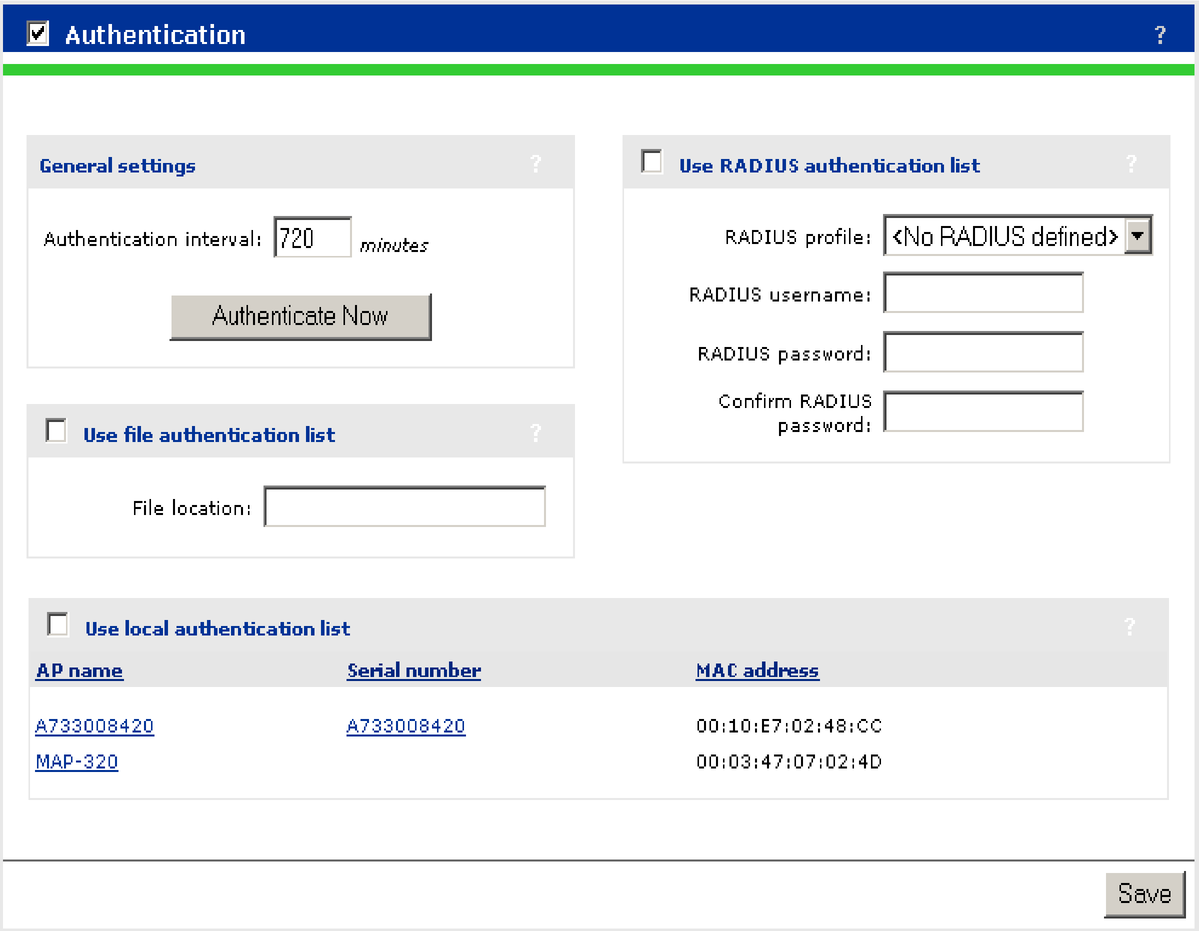
- **Already Seen**: The AP established a control channel to the service controller at least once in the past.

4.5 Authentication of Controlled APs

For security purposes, the service controller can require that APs be authenticated before they are managed. Authentication is enabled by selecting **Service controller >> Controlled APs > Authentication.**

NOTE

The AP authentication option is disabled by default, meaning that all discovered APs are authorized (no authentication is required).



☑ Authentication

General settings

Authentication interval: 720 minutes

□ Use file authentication list

File location:

□ Use RADIUS authentication list

RADIUS profile: <No RADIUS defined>

RADIUS username:

RADIUS password:

Confirm RADIUS password:

□ Use local authentication list

AP name	Serial number	MAC address
A733008420	A733008420	00:10:E7:02:48:CC
MAP-320		00:03:47:07:02:4D

Figure 4-6: Controlled APs - Authentication

The service controller authenticates APs using their MAC addresses. When an AP sends a discovery request to the service controller, it includes its Ethernet Base MAC address. The service controller validates this address against its AP address authentication list. If the address appears in the list, the AP is authenticated and gains access to the service controller's service control features.

If authentication fails (for example, this is a new AP), and the **Use the local authentication list** option is enabled, then the AP is added to the **Default Group** and flagged as requiring authentication. The AP must then be manually authenticated by the administrator using the **Controlled APs** >> **Overview** > **Discovered APs** page. Once authenticated, the AP can be managed.

NOTE

APs remain visible in this list as long as they have been detected and authorized at least once. If an AP is no longer part of the network then the administrator must manually remove it.

4.5.1 Building the AP Authentication List

The service controller can retrieve authentication list entries from several sources: a RADIUS account, a file, or using the set of locally configured APs. All entries are merged to create a combined list.

The service controller retrieves authentication list entries when:

- the **Authentication interval** expires
- **Authenticate Now** is clicked
- **Save** is clicked
- each time the service controller starts up

Each time the authentication list entries are retrieved all connected APs are checked against it. If an AP's MAC address is no longer listed, its connection is terminated.

NOTE

Although the same RADIUS account can be shared between this option and the **Public access > Attributes** page, it is recommended that a separate RADIUS account be created for each option.

4.5.1.1 General Settings

- Authentication Interval

  Specifies the interval at which the service controller retrieves authentication list entries from the selected authentication sources. After the entries are retrieved all controlled APs are evaluated against the new list.

- Authenticate Now

  Causes the service controller to retrieve authentication list entries from all selected sources.

4.5.1.2 Use File Authentication List

When this option is selected, the service controller retrieves authentication list entries from a file. This must be an ASCII file with one or more MAC addresses in it. Each address must be entered on a separate line. For example:

```
00:03:52:00:00:01
00:03:52:00:00:02
00:03:52:00:00:03
```

A label affixed to each AP indicates its Ethernet Base MAC Address. This is the address to specify in the authentication list.

4.5.1.2.1 File Location

Specify the location of the file to use for authentication of APs using either HTTP or FTP. For example:

ftp://mydomain.com/auth_list
ftp://*username*:*password*@mydomain.com/auth_list

http://mydomain.com/auth_list

4.5.1.2.2 Use RADIUS Authentication List

When this option is selected, the service controller retrieves authentication list entries from a RADIUS server. List entries must be defined in the RADIUS account for the service controller using the following Alvarion-AVPair value string:

`managed-map=`*MAC_address*

Where *`MAC_address`* is the Ethernet Base port MAC address of the controlled AP (which is printed on a sticker affixed to the AP’s case). Use colons to separate characters in the address.

For example: `00:20:E0:6B:4B:44`.

To define multiple addresses, specify additional entries as needed.

This attribute conforms to RADIUS RFC 2865. You may need to define this attribute on your RADIUS server if it is not already present as follows:

- SMI network management private enterprise code = 8744

- Vendor-specific attribute type number = 0

- Attribute type = string

4.5.1.2.2.1 RADIUS Profile

When the **Authentication** source is **RADIUS**, this option specifies the name of the RADIUS profile to use. There is no default. To configure RADIUS profiles, select **Security** > **RADIUS**.

4.5.1.2.2.2 RADIUS Username

When the **Authentication** source is **RADIUS**, specifies the RADIUS username assigned to the service controller.

4.5.1.2.2.3 RADIUS Password / Confirm RADIUS Password

Specifies the password that corresponds with **RADIUS username**.

4.5.1.3 Use the Local Authentication List

When this option is selected, the service controller creates authentication list entries based on the set of APs that are currently defined on the service controller. For reference purposes, the table shows the **AP name**, **Serial number** and **MAC address** of all APs that are defined and will be included in the authentication list.

NOTE

When the local authentication list is enabled, the first time an AP tries to connect to the service controller an administrator must manually accept the AP on the **Controlled APs >> Overview > Discovered APs** page. Otherwise, the AP will not be able to connect to the service controller.

4.6 Configuring APs

This section explains how to manage AP configuration using the service controller's management tool.

4.6.1 Overview

AP configuration can be done at the Controlled APs level, group-level, or AP-level.

- **Group-level configuration** enables you to define settings that are shared by APs with similar characteristics. For example, if you have several APs at a location that are all providing the same service, putting them in the same group makes them easier to manage.

- **AP-level configuration** enables you to specify configuration settings for a particular AP that overrides corresponding group-level settings.

NOTE

Assignment of virtual networks is only done at the group-level. This means that all APs in a group always have the same virtual network settings.

4.6.1.1 Viewing Groups and APs

Groups and APs are displayed in the **Network tree** under **Controlled APs**. For example:

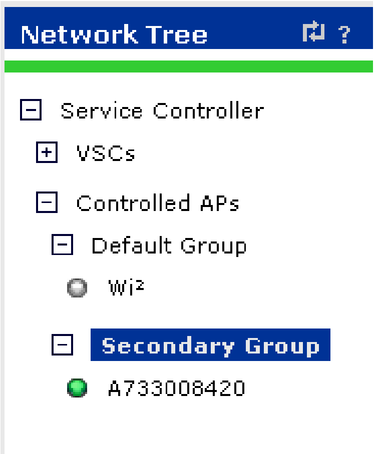


Figure 4-7: Controlled APs Menu

Click the **+** symbol next to **Controlled APs** to expand the tree to see all groups. Click the **+** symbol next to each group to see its APs.

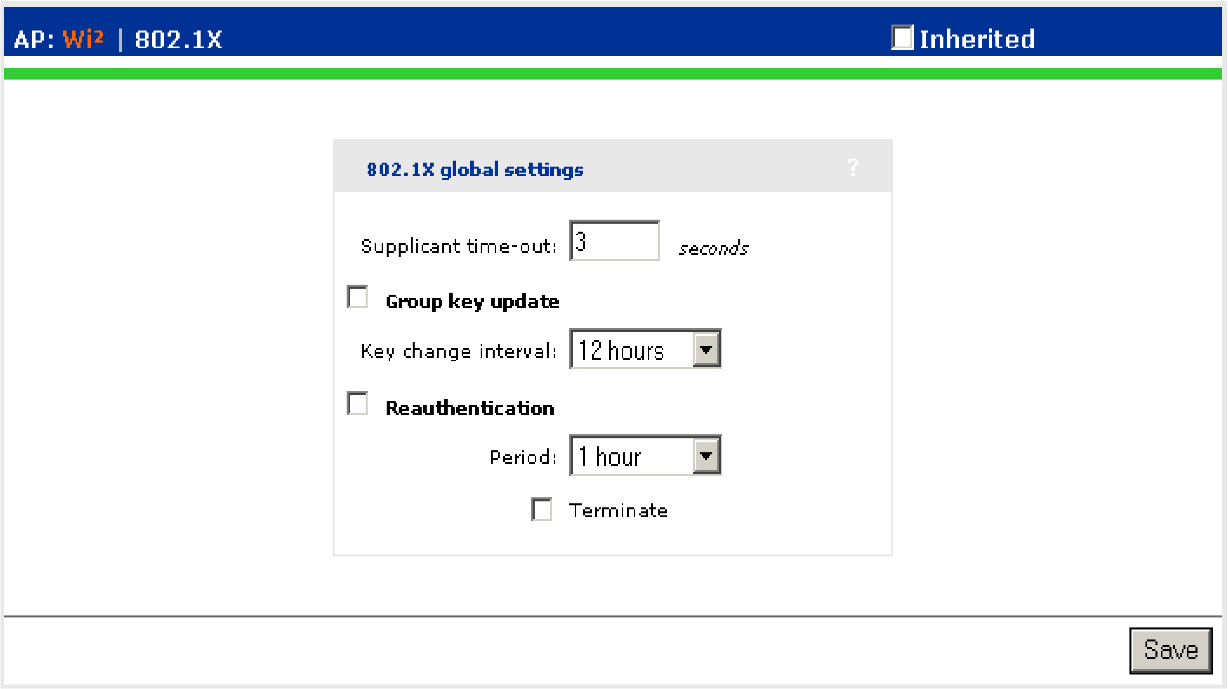
The **Default Group** is always present. All newly-discovered APs are initially placed in this group. Additional groups (**Secondary Group**, in this example**)**, can be added and have APs assigned to them.

4.6.1.2 Inheritance

To make configuration of groups and APs easier, configuration settings are inherited as follows:

- Settings made at the **Controlled APs** level are inherited by all groups.
- Settings made at the **Group** level are inherited by all the APs in a group.

To change inherited configuration settings you must first clear the **Inherited** checkbox. For example, the following image shows the **802.1X** page with the **inherited checkbox** cleared, allowing all settings on this page to be customized.



AP: Wi² | 802.1X

□ Inherited

802.1X global settings

Supplicant time-out: 3 seconds

□ Group key update

Key change interval: 12 hours

□ Reauthentication

Period: 1 hour

□ Terminate

Figure 4-8: Inheritance Feature

4.6.1.3 Binding Virtual Networks to Groups

The service controller defines a global pool of virtual networks ("Working with Virtual Networks" on page 97) that represents the services that are available on the network. From this pool, specific virtual networks can be *bound* to one or more groups (and the APs in the groups), to provide a homogeneous wireless offering.

Any changes to a bound virtual network affect all groups (and APs) to which the virtual network is bound, making it easy to manage configuration changes network-wide.

4.6.1.4 Synchronizing APs

After making configuration changes to an AP or a group, you must update all controlled APs with the new settings by synchronizing them. For more information, see "Synchronizing APs" on page 72.

4.6.2 Configuration Strategy

There are two ways to approach AP configuration:

4.6.2.1 Discover APs and then Configure Groups

This strategy works as follows:

1. Deploy the APs in their default configuration on the network.
2. Allow the discovery process to find the APs and place them in the default group.
3. Create group definitions and then move the APs to the appropriate group.

4.6.2.2 Configure Groups and then Discover APs

This strategy works as follows:

1. Create group definitions.
2. Manually define each AP in the appropriate group.
3. Deploy the APs in their default configuration on the network.
4. Allow the discovery process to find the APs and place them in the pre-configured groups.

4.6.3 Working with Groups

4.6.3.1 Adding a New Group

To create a new group, do the following:

1. Select **Controlled APs** >> **Group management**.

2 Select **Add New Group**.

3 Specify the name of the new group and select **Save**.

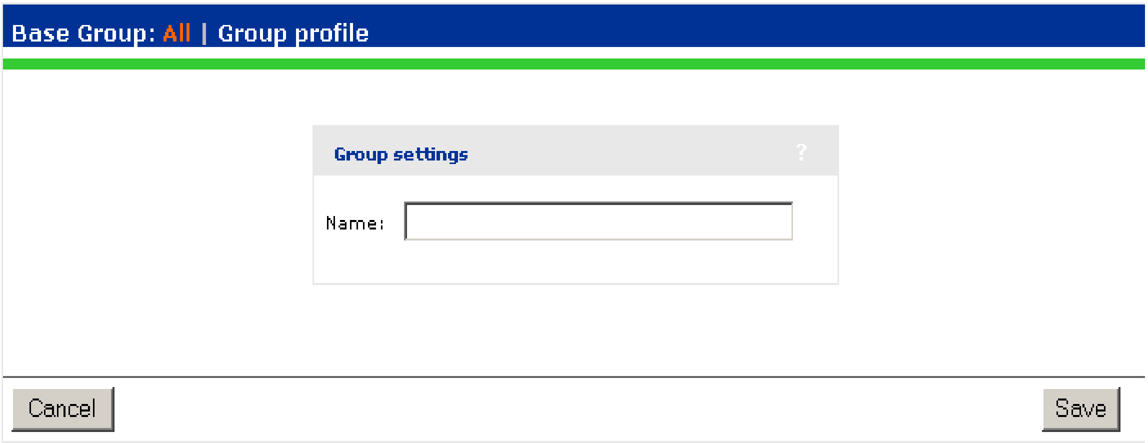


Figure 4-9: Adding a New Group

4.6.3.2 Deleting a Group

NOTE

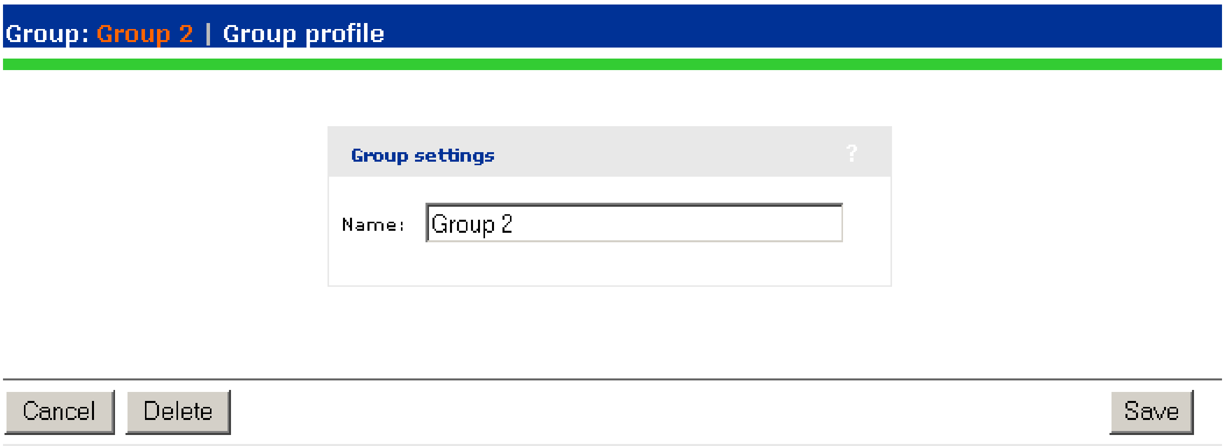
You must remove all APs from a group before you delete it.

To delete a group, do the following:

1 Select **Controlled APs >> Group management**.

2 Select the name of the group you want to delete.

3 Select **Delete**.



Group: Group 2 | Group profile

Group settings

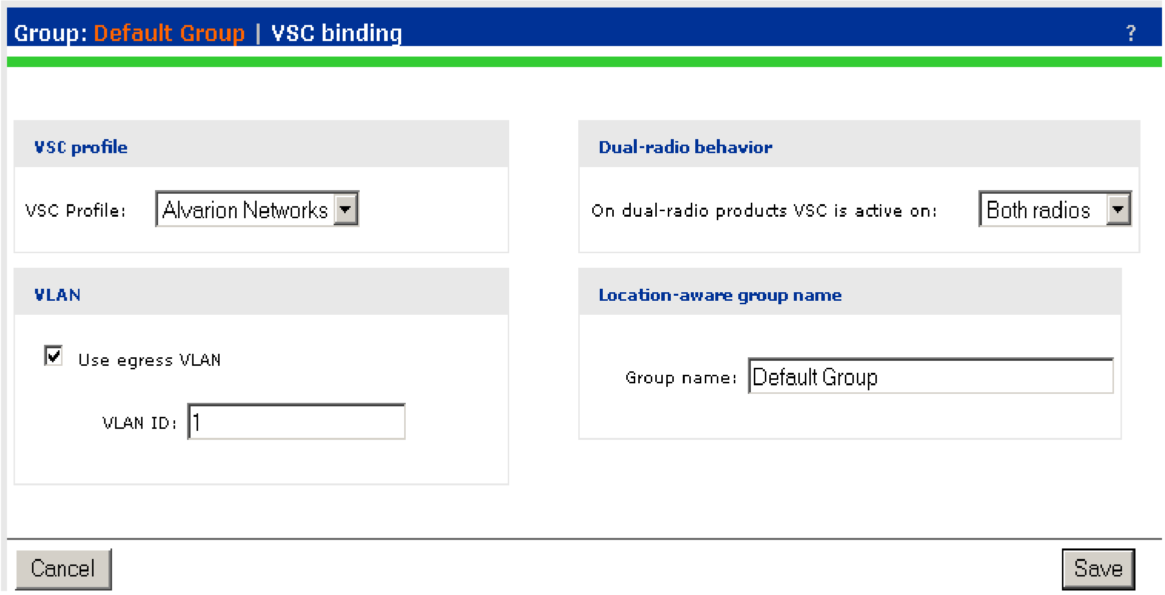
Name: Group 2

Figure 4-10: Deleting a Group

4.6.3.3 Binding a Virtual Network to a Group

To bind a virtual network to a group, do the following:

1. Select the target group under **Controlled APs**.
2. In the right pane, select **VSC bindings**, then select **Add New Binding**.



Group: Default Group | VSC binding

VSC profile

VSC Profile: Alvarion Networks

Dual-radio behavior

On dual-radio products VSC is active on: Both radios

VLAN

☑ Use egress VLAN

VLAN ID: 1

Location-aware group name

Group name: Default Group

Figure 4-11: Binding a Virtual Network to a Group

3. Select the **VSC profile** and define other configuration settings as required.
4. Select **Save**.

4.6.4 Working with APs

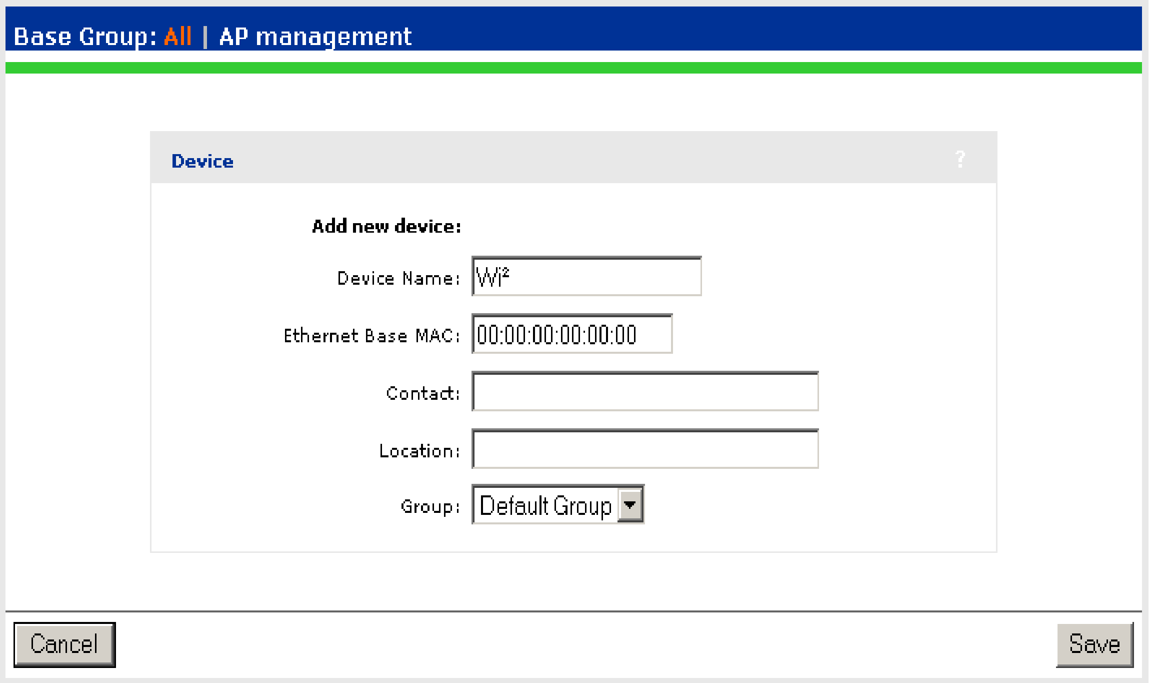
4.6.4.1 Manually Adding a New AP

You can manually add APs to the service controller before connecting the APs to the network. This is useful, for example, when you want to pre-designate the group into which an AP will be placed.

1 Select **Controlled APs >> Overview > Configured APs**.

2 Select **Add**.

3 In the **Device** box, identify the new AP, specifying at a minimum, **Device Name**, **Ethernet BASE MAC** (printed on the label affixed to each AP), and **Group**.



Add new device:

Device Name: Wi^2

Ethernet Base MAC: 00:00:00:00:00:00

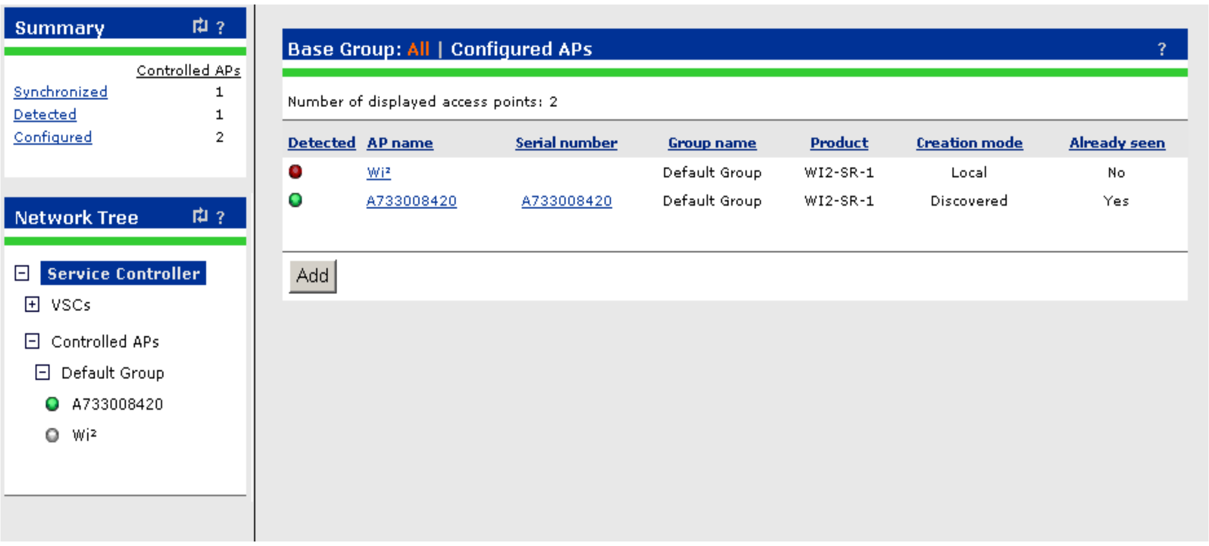
Contact:

Location:

Group: Default Group

Figure 4-12: Adding a New AP

Select **Save**. The AP is added to the selected group in the Network tree and will also be shown in the Configured APs list.



	Controlled APs
Synchronized	1
Detected	1
Configured	2

Base Group: All | Configured APs

Number of displayed access points: 2

Detected	AP name	Serial number	Group name	Product	Creation mode	Already seen
●	Wi²		Default Group	WI2-SR-1	Local	No
●	A733008420	A733008420	Default Group	WI2-SR-1	Discovered	Yes

Figure 4-13: Configured APs List

NOTE

When the AP is physically connected to the network, it will discover the service controller and automatically be accepted into the selected group. Make sure you configure the correct MAC address, otherwise the AP will just be discovered as a new AP and will not be placed into the selected group.

NOTE

If an AP is created with the wrong product type it will go into the **Wrong product** state when discovered. (For example, if you specify AP-330 for an AP that is an AP-320.) To remedy this, select **Overview > Discovered APs** and select the **Accept Products** link in the **Action** column. (This action will override the pre-configured product setting by the information discovered from the actual physical AP.)

4.6.4.2 Deleting an AP

1. To delete an AP, select the AP in the **Network tree**, and then in the **Configured APs** list, select the AP’s name in the **Link** column.
2. On the **AP management** page, select **Delete**. The AP is deleted.

NOTE

When the AP authentication feature is disabled, a deleted AP may automatically rediscover the service controller if the AP is left connected to the network. Therefore, immediately after deletion, disconnect the AP unless you want it to rediscover the service controller.

4.6.4.3 Moving an AP to a Different Group

NOTE

Moving an AP to a different group causes it to be restarted.

4.6.4.3.1 Using Drag-and-drop

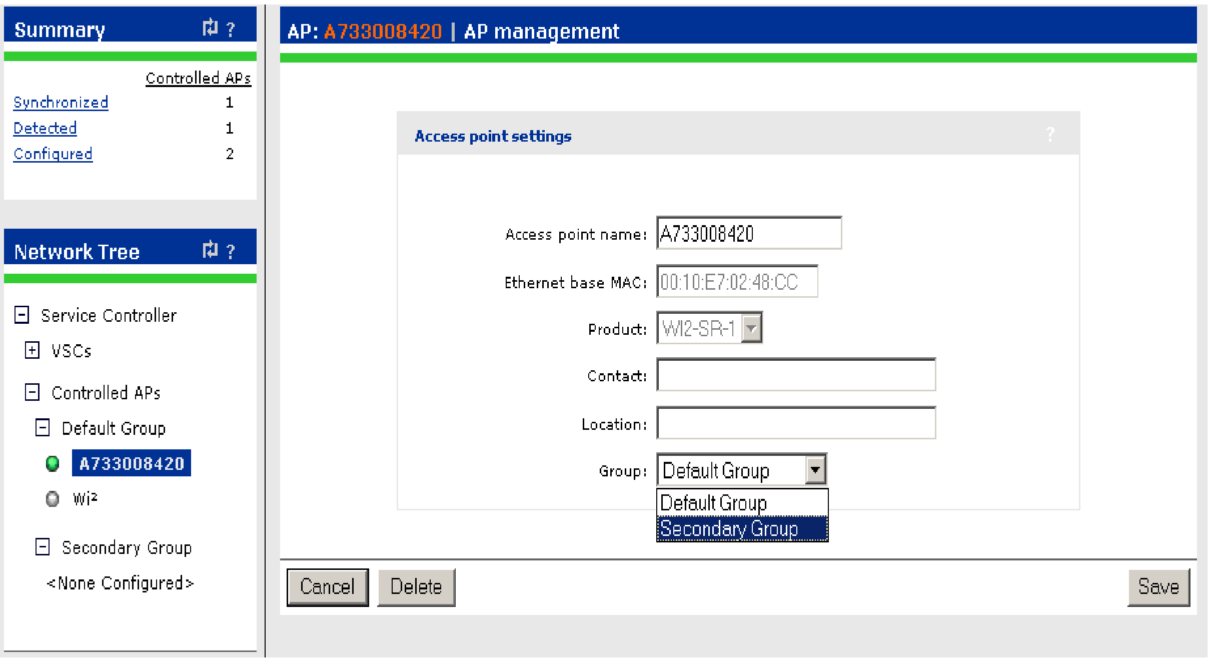
The easiest way to move an AP to a different group is to drag-and-drop it from the old group to the new group. Both groups must be visible in the Network tree for this to work.

The move to the different group does not actually occur until the AP is synchronized as described in the next section, Synchronizing APs.

4.6.4.3.2 Using Menus

1 In the **Network tree** select the AP and then on the main menu, select **Device Management** > **AP management**.

2 Under **Access point settings**, select the desired **Group** and select **Save**.



Access point name: A733008420
Ethernet base MAC: 00:10:E7:02:48:CC
Product: WI2-SR-1
Contact:
Location:
Group: Default Group
Default Group
Secondary Group

Figure 4-14: Selecting a Group

This puts the AP into the unsynchronized state (it will be displayed in orange).

The move does not occur until the AP is synchronized as described in the next section, Synchronizing APs.

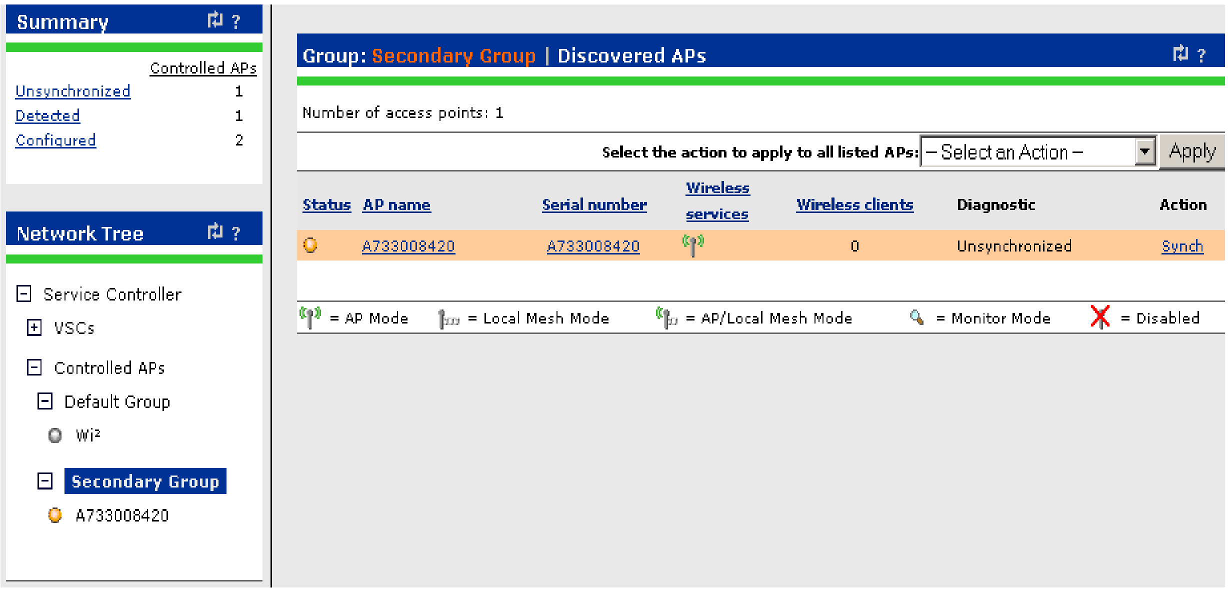
4.6.4.4 Synchronizing APs

NOTE

Depending on the type of configuration changes that are being synchronized, wireless users may be forced to reassociate or login again.

After making configuration changes, you must synchronize the APs with the updated configuration as follows:

1 In the **Network tree**, select the group that contains the APs. For example, **Secondary Group**.



	Controlled APs
Unsynchronized	1
Detected	1
Configured	2

Group: Secondary Group | Discovered APs

Number of access points: 1

Select the action to apply to all listed APs: -- Select an Action --

Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
●	A733008420	A733008420		0	Unsynchronized	Synch

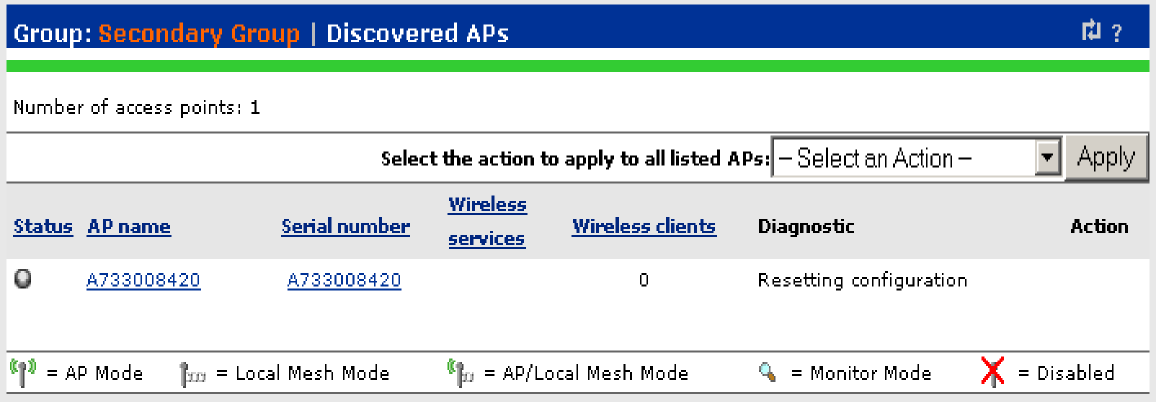
Figure 4-15: Synchronizing APs - 1

APs requiring synchronization are displayed with an orange background and show **Unsynchronized** in the **Diagnostic** column.

2 Select a **Synch** link in the **Action** column to synchronize a single AP.

Or, to synchronize all unsynchronized APs in the group, select **Synchronize Configuration** in the **Select the action to apply to all listed APs** list, and select **Apply**.

3 Monitor synchronization progress by watching the **Diagnostic** column. Messages such as **Resetting configuration** and **Restoring configuration** will appear during the synchronization process.



Group: Secondary Group | Discovered APs

Number of access points: 1

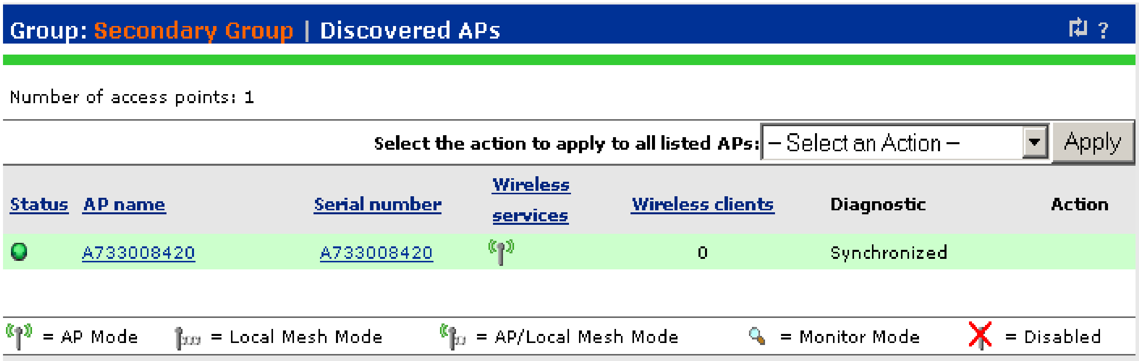
Select the action to apply to all listed APs: – Select an Action – Apply

Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
●	A733008420	A733008420		0	Resetting configuration	

= AP Mode = Local Mesh Mode = AP/Local Mesh Mode = Monitor Mode = Disabled

Figure 4-16: Synchronizing APs - 2

4 As each synchronization completes, the **Status** light and background color of the synchronized AP changes to green. The status light next to the AP name under the pertinent group name in the Network tree also changes to green. This indicates that the AP is fully operational and using its new configuration.



Group: Secondary Group | Discovered APs

Number of access points: 1

Select the action to apply to all listed APs: – Select an Action – Apply

Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
●	A733008420	A733008420		0	Synchronized	

= AP Mode = Local Mesh Mode = AP/Local Mesh Mode = Monitor Mode = Disabled

Figure 4-17: Synchronizing APs - 3

4.7 Defining VLANs

TIP

This section describes how to assign an egress VLANs to controlled APs. For information on the service controller’s VLAN implementation, see “VLAN support” on page 112.

Each time a virtual network is bound to a group, you have the option of assigning a VLAN ID to be used for egress traffic sent by all APs in the group.

For example, if virtual network 1 and virtual network 2 are both bound to the Default Group, the egress traffic for each virtual network could be tagged with a different VLAN to segregate the traffic.

NOTE

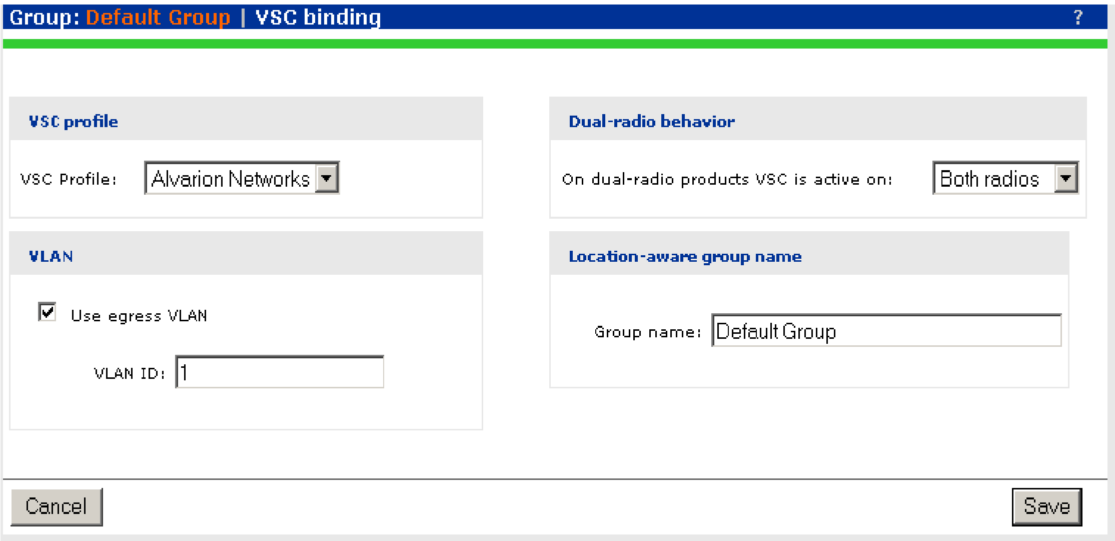
If a RADIUS attribute is being used to assign a VLAN ID to a user, then the RADIUS VLAN assignment overrides the VLAN assigned on this page.

To define an egress VLAN as follows:

1 Select the target group under **Controlled APs**.

2 In the right pane, select **VSC bindings** and then select a binding in the list.

3 Select the **Use egress VLAN** checkbox and then specify a **VLAN ID**.



VSC Profile: Alvarion Networks

On dual-radio products VSC is active on: Both radios

☑ Use egress VLAN

VLAN ID: 1

Group name: Default Group

Figure 4-18: Defining VLANs

4 Select **Save**.

4.8 Provisioning

Provisioning is the means by which you can change the factory default IP addressing method and service controller discovery settings on controlled APs.

Provisioning is generally not required when deploying controlled APs in simple network topologies. However, it is required when controlled APs:

- do not have layer 2 connectivity to a service controller and where it is not possible to control the DNS or DHCP server configuration. For more information, see “Discovery Recommendations” on page 45.
- need to be deployed with static IP addresses
- use a local mesh to connect to the service controller. For more information, see “Provisioning Local Mesh Links” on page 306.

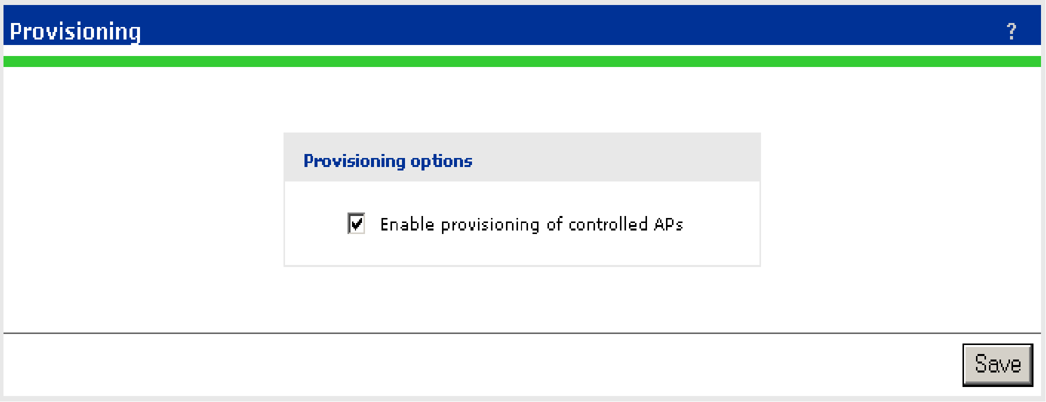
4.8.1 Provisioning Methods

Provisioning can be done in two ways:

- **Use the** service controller **to provision controlled APs:** On the service controller, provisioning can be done at the group or AP level for added flexibility. Provisioning via the service controller is the preferred method.

In certain scenarios it may be practical to use one service controller to provision APs, and then have the APs associate with another service controller after being deployed. For example, provisioning could occur at the network operations center by connecting APs to the same subnet as a service controller. Once provisioned, the APs could then be deployed in the field where they would discover a service controller that is already in operation.

To enable a service controller to send provisioned settings to controlled APs, you must first activate the **Enable provisioning of controlled APs** option on the **Service Controller** >> **Controlled APs** > **Provisioning** page.



Provisioning options

☑ Enable provisioning of controlled APs

Figure 4-19: Enabling Provisioning

NOTE

Until this option is enabled, provisioned settings defined on the service controller are not sent to any controlled APs.

After an AP has been updated with provisioned settings, these settings do not become active until the AP is restarted, or a **Remove and rediscover** action is executed on the **Controlled APs** >> **Configured APs** page.

- **Directly provision an AP using its management tool:** In its factory default state, the AP provides a provisioning menu with the same options that are available on the service controller. Use this method when there is no local service controller on which to perform the provisioning.

NOTE

Once a AP has established the secure management tunnel with a service controller the provisioning menu on the AP is no longer accessible.

In both cases, the configuration settings that you have access to are the same. They are described in the following sections.

CAUTION

Provisioned settings on the service controller always overwrite provisioned settings defined directly on an AP. If the wrong configuration settings are defined on the service controller and applied to an AP, it can cause the AP to lose contact with the network.

4.8.2 Displaying the Provisioning Pages

To display the provisioning pages, do the following:

4.8.2.1 On a Service Controller

1 Select one of the following in the Network tree:

- » Controlled APs
- » A group
- » A AP

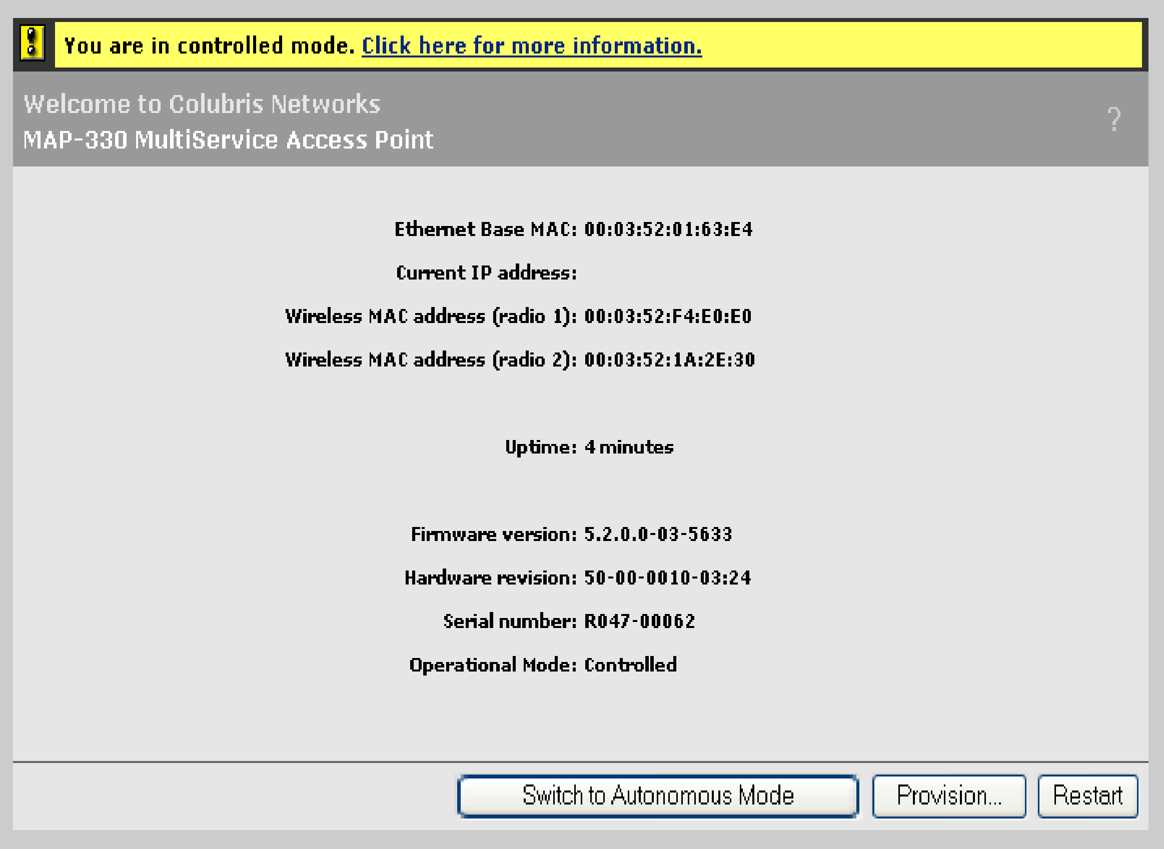
2 In the right pane, select **Provisioning** > **Connectivity**.

3 Configure provisioning settings as described in the sections that follow.

4.8.2.2 On an AP

1 Login to its management tool.

2 Select **Provision** at the bottom of the home page.



You are in controlled mode. Click here for more information.

Welcome to Colubris Networks
MAP-330 MultiService Access Point

Ethernet Base MAC: 00:03:52:01:63:E4

Current IP address:

Wireless MAC address (radio 1): 00:03:52:F4:E0:E0

Wireless MAC address (radio 2): 00:03:52:1A:2E:30

Uptime: 4 minutes

Firmware version: 5.2.0.0-03-5633

Hardware revision: 50-00-0010-03:24

Serial number: R047-00062

Operational Mode: Controlled

Figure 4-20: HomePage Window

NOTE

The **Provision** button is only available if the AP is in its factory-default state, meaning it has not yet been provisioned and that the AP has never discovered a service controller (since last factory default). To force an AP into its factory-default state, press and hold its reset button until all lights flash on and off three times.

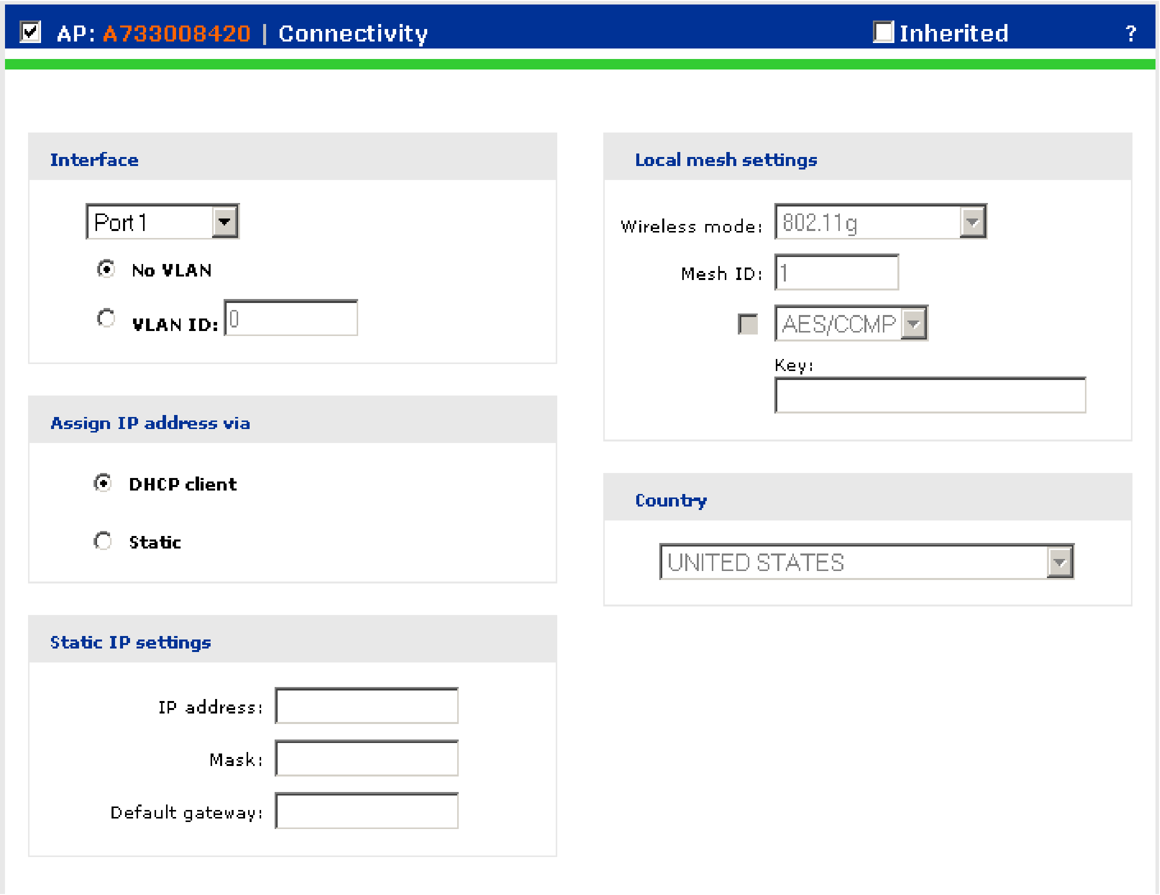
3 Configure provisioning settings as described in the sections that follow.

4.8.3 Provisioning Connectivity

Use the **Provisioning** > **Connectivity** page to provision connectivity and local mesh settings for a controlled AP. The following options can be provisioned: interface through which discovery is attempted, addressing method (DHCP or static), as well as local mesh settings.

NOTE

To enable provisioning, make sure that you select the checkbox in the top left corner.



☑ AP: A733008420 | Connectivity □ Inherited ?

Interface

Port 1

● No VLAN

○ VLAN ID: 0

Assign IP address via

● DHCP client

○ Static

Static IP settings

IP address:

Mask:

Default gateway:

Local mesh settings

Wireless mode: 802.11g

Mesh ID: 1

□ AES/CCMP

Key:

Country

UNITED STATES

Figure 4-21: Provisioning Connectivity

4.8.3.1 Interface

Select the interface you want to configure and then define its settings using the other options on this page. Set **VLAN ID** if applicable.

NOTE

Certain parameters can only be set at the device-level.

4.8.3.2 Assigning an IP Address

Assign an IP address via:

- **DHCP client:** Address is assigned using a DHCP server. Enable this option to have the interface act as a DHCP client. The AP sends DHCP requests on the specified VLAN. If no VLAN is specified, the request is sent untagged.

- **Static:** Select this option to manually assign an IP address to the interface.

4.8.3.3 Static IP Settings

When you select **Static** for **Assign IP address via**, configure settings in this box.

- **IP address:** Specify the IP address you want to assign to the interface.
- **Address mask:** Specify the appropriate subnet mask for the IP address you specified.
- **Default gateway:** Specify the IP address of the default gateway.

4.8.3.4 Local Mesh Settings

For information on provisioning these settings, refer to "Local Mesh" on page 291.

4.8.4 Provisioning Discovery

Use the **Provisioning > Discovery** page to provision the method a controlled AP uses to discover a service controller. Two options can be provisioned: DNS discovery or discovery via IP address. The following page shows Discovery using DNS provisioned.

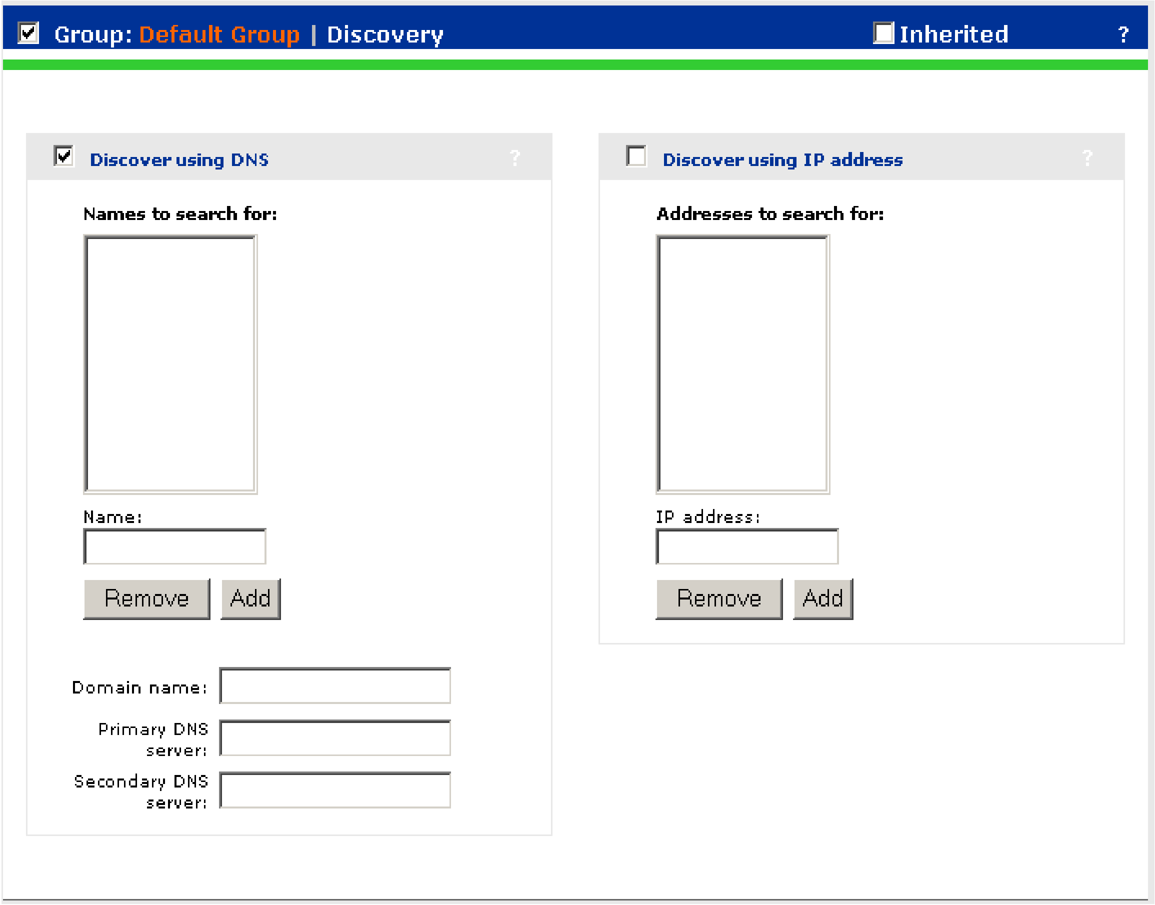


Figure 4-22: Provisioning Discovery

4.8.4.1 Discover Using DNS

The AP attempts to connect with a service controller using the names in the order that they appear in this list.

To discover the service controller on the network, the AP appends each name with the specified **Domain name**.

In the above example, the AP will search for service controllers with the names:

- service-controller-1.mydomain.com
- service-controller-2.mydomain.com

If you define a name that contains a dot, then the domain name is not appended . For example, if the name is **controller.yourdomain.com**, no domain name is appended.

If the AP is operating as a DHCP client, the DHCP server will generally return a domain name when it assigns an IP address to the AP. If you leave the **Domain name** field on this page blank, then the DHCP domain name is appended to the specified names instead.

4.8.4.2 Discover Using IP Address

The AP attempts to connect with a service controller using the IP addresses in the order that they appear in this list.

4.8.5 Provisioning Summary

The following table defines the potential outcome for all provisioning scenarios.

Connectivity provisioned	Discovery provisioned	Result
No	No	Default behavior is used for connectivity and discovery. See “Discovery of Controlled APs” on page 42.
No	Yes	Discovery occurs using the provisioned methods on the following interfaces: Last interface on which a service controller was discovered. (Only applies to APs that have previously discovered a service controller.) Untagged on port 1. All detected VLANs (in sequence) on port 1.
Yes	No	Discovery methods are used according on the provisioned connectivity settings. See “Discovery of Controlled APs” on page 42. DHCP discovery is not executed if a static IP address is provisioned.
Yes	Yes	Discovery occurs using the provisioned methods over the provisioned connectivity. The provisioned discovery method is retried indefinitely if it fails, however other discovery methods are not attempted.

4.9 Firmware Retrieval/Update

Firmware management of controlled APs is automatically performed by the service controller after the AP is discovered (“Key Controlled-mode Events” on page 40).

If the firmware version on the AP does not match the version installed on the service controller, new firmware is installed on the AP by the service controller.

For information on how to update the service controller firmware see “Firmware Updates” on page 341.

4.10 Monitoring

The service controller provides a series of pages that present monitoring and status information for controlled APs. You can view these pages for all controlled APs, for all APs in a group, or for just a specific AP. All options appear on the **Overview** menu, which can be reached by selecting:

- **Controlled APs** >> **Overview**.
- **Controlled APs** > **[Group name]** >> **Overview**.
- **Controlled APs** > **[Group name]** > **[AP name]** >> **Overview**.

Consult the online help for details about the information provided on these status pages.

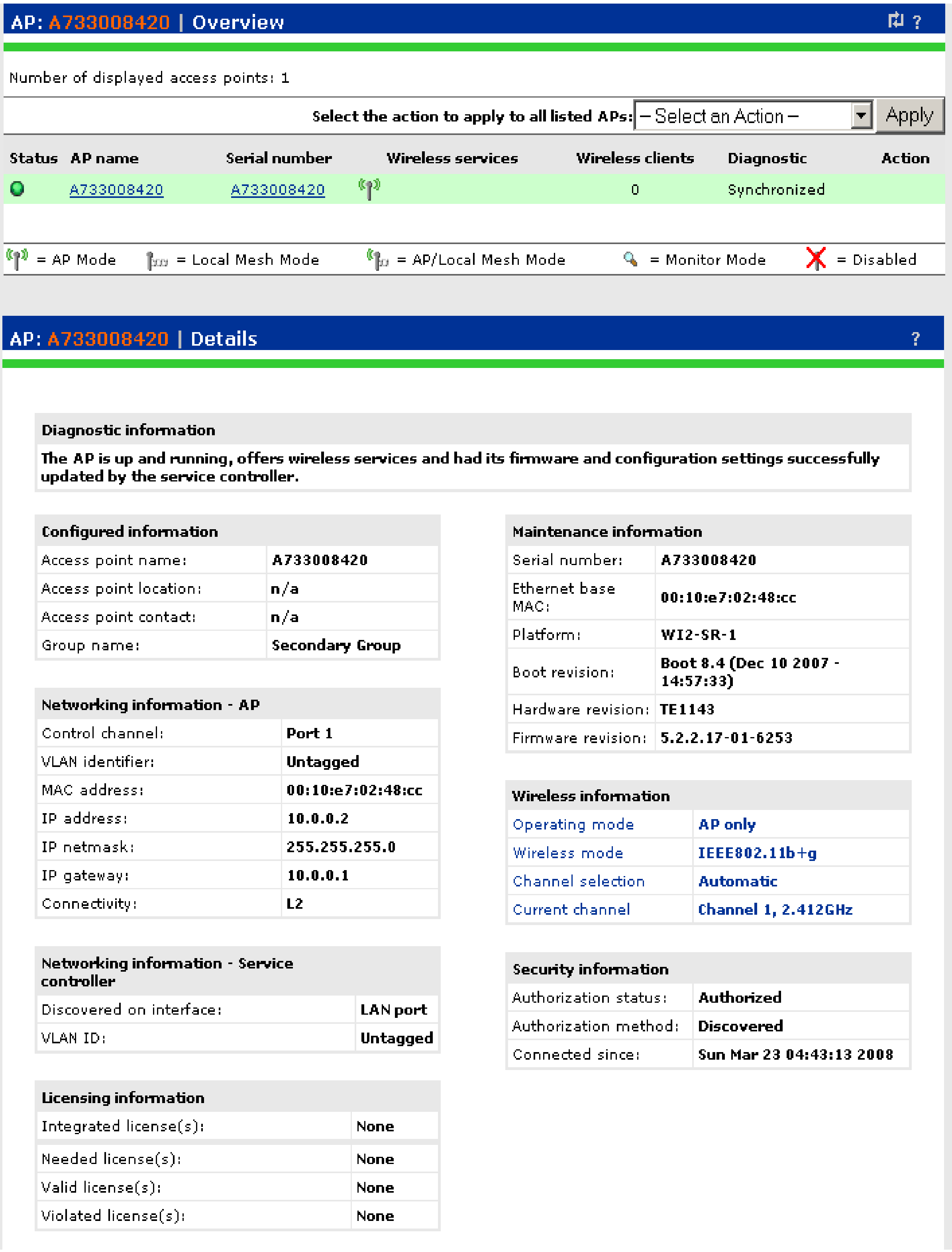
4.10.1 Overview Menu

The Overview menu organizes monitoring information with one page per item as follows:

- “AP Details” on page 85
- “Wireless Clients” on page 89
- “Wireless Rates” on page 91
- “Neighborhood” on page 92
- “Mobility Neighbors” on page 93
- “Local Mesh Neighborhood” on page 94
- “Local Mesh Links” on page 95
- “Licenses” on page 95

4.10.2 AP Details

To display detailed information for a specific AP, select the AP name under **Controlled APs** in the Network tree, and then select **Overview** > **AP details**.



AP: A733008420 | Overview

Number of displayed access points: 1

Select the action to apply to all listed APs: – Select an Action – Apply

Status	AP name	Serial number	Wireless services	Wireless clients	Diagnostic	Action
●	A733008420	A733008420		0	Synchronized	

= AP Mode   = Local Mesh Mode   = AP/Local Mesh Mode   = Monitor Mode   ✗ = Disabled

AP: A733008420 | Details

Diagnostic information

The AP is up and running, offers wireless services and had its firmware and configuration settings successfully updated by the service controller.

Configured information	
Access point name:	A733008420
Access point location:	n/a
Access point contact:	n/a
Group name:	Secondary Group

Networking information - AP	
Control channel:	Port 1
VLAN identifier:	Untagged
MAC address:	00:10:e7:02:48:cc
IP address:	10.0.0.2
IP netmask:	255.255.255.0
IP gateway:	10.0.0.1
Connectivity:	L2

Networking information - Service controller	
Discovered on interface:	LAN port
VLAN ID:	Untagged

Licensing information	
Integrated license(s):	None
Needed license(s):	None
Valid license(s):	None
Violated license(s):	None

Maintenance information	
Serial number:	A733008420
Ethernet base MAC:	00:10:e7:02:48:cc
Platform:	WI2-SR-1
Boot revision:	Boot 8.4 (Dec 10 2007 - 14:57:33)
Hardware revision:	TE1143
Firmware revision:	5.2.2.17-01-6253

Wireless information	
Operating mode	AP only
Wireless mode	IEEE802.11b+g
Channel selection	Automatic
Current channel	Channel 1, 2.412GHz

Security information	
Authorization status:	Authorized
Authorization method:	Discovered
Connected since:	Sun Mar 23 04:43:13 2008

Figure 4-23: AP Details

TIP

For information on the content of the **Overview** box, see “Viewing all Discovered APs” on page 53.

The **Details** box provides this information:

- **Diagnostic information**: Provides more detailed information for any message that appears in the Overview Diagnostic column.
- **Configured information**
  - **Access point name**: Name assigned to the AP.
  - **Access point location**: Location information assigned when the AP was defined.
  - **Access point contact**: Contact information assigned when the AP was defined.
  - **Group name**: Group to which the AP is assigned.
- **Networking information - AP**
  - **Control channel**: Interface the AP is using to communicate with the service controller.
  - **VLAN identifier**: VLAN the AP is using to communicate with the service controller.
  - **MAC address**: MAC address of the AP Port used to communicate with the service controller.
  - **IP address**: IP address of the AP Port used to communicate with the service controller.
  - **IP netmask**: Network mask associated with the IP address.
  - **IP gateway**: Address of the gateway assigned to the AP.
  - **Connectivity**: Indicates the network connectivity detected between the service controller and the AP. Values can be L2, L3, or L3+NAT.
- **Networking information - Service controller**

  - **Discovered on interface**: The service controller Interface on which the AP was discovered.
  - **VLAN ID**: The local VLAN identifier on the service controller on which the AP was discovered. (Specifies “Untagged” if no VLAN.)

- **Licensing information**
  - **Integrated license(s)**: Licenses that are installed on the AP.
  - **Needed license(s)**: Licenses that are required to support the features configured on the AP.
  - **Valid license(s)**: Valid licenses that the AP actually uses from the Needed licenses list.
  - **Violated license(s)**: The AP cannot be configured with a needed license because it is not installed on the AP or not installed on the service controller or it has expired.

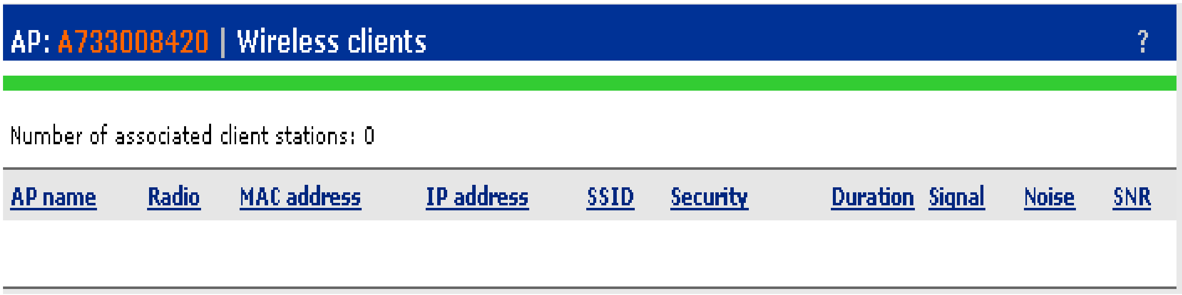
- **Maintenance information**
  - **Serial number**: AP's serial number. Also available on the label affixed to the AP.
  - **Ethernet base MAC**: AP's base MAC address. Also available on the label affixed to the AP.
  - **Platform**: AP's product type.
  - **Boot revision**: Version number of the AP's boot software.
  - **Hardware revision**: Version number of the AP's hardware.
  - **Firmware revision**: Version number of the firmware currently loaded on the AP.

- **Wireless information**
  - **Operating mode**: Mode the AP is currently operating in. Possible values are:
    - **Access point only**: Provides AP functionality only. Wireless links cannot be created.

    - ◇ **Monitor**: Indicates if monitor functions are enabled/disabled. When enabled, monitoring disables AP functions. Provides continual scanning across all channels in all wireless modes (a/b/g).
    - ◇ **Sensor**: Indicates if RF sensor functionality is enabled/disabled. This feature requires that the appropriate license is installed either directly on the AP or as a group license on the service controller.
    - ◇ **Local mesh**: Indicates is local mesh is enabled/disabled.
    - ◇ **Access point and local mesh**: Indicates if support for both AP and local mesh functions are enabled.
  - » **Wireless mode**: Indicates the transmission speed and frequency band provided by the AP. Possible values are:
    - ◇ 802.11b: 11 Mbps in the 2.4 GHz frequency band
    - ◇ 802.11b + 802.11g: 11 and 54 Mbps in the 2.4 GHz frequency band
    - ◇ 802.11g: 54 Mbps in the 2.4 GHz frequency band
  - » **Channel selection**: Indicates whether the channel is automatically selected or statically configured.
  - » **Current channel**: Wireless channel the AP is currently operating on.
- **Security information**
  - » **Authorization status**: Indicates if the AP has be authenticated by the service controller.
  - » **Authorization method**: Method used to authenticate the AP.
  - » **Connected since**: Indicates the date and time the AP last connected.

4.10.3 Wireless Clients

You can view information about wireless users that are associated with a specific controlled AP, all controlled APs, or a specific group of controlled APs by selecting **Overview** > **Wireless clients** in the right pane.



AP: A733008420 | Wireless clients ?

Number of associated client stations: 0

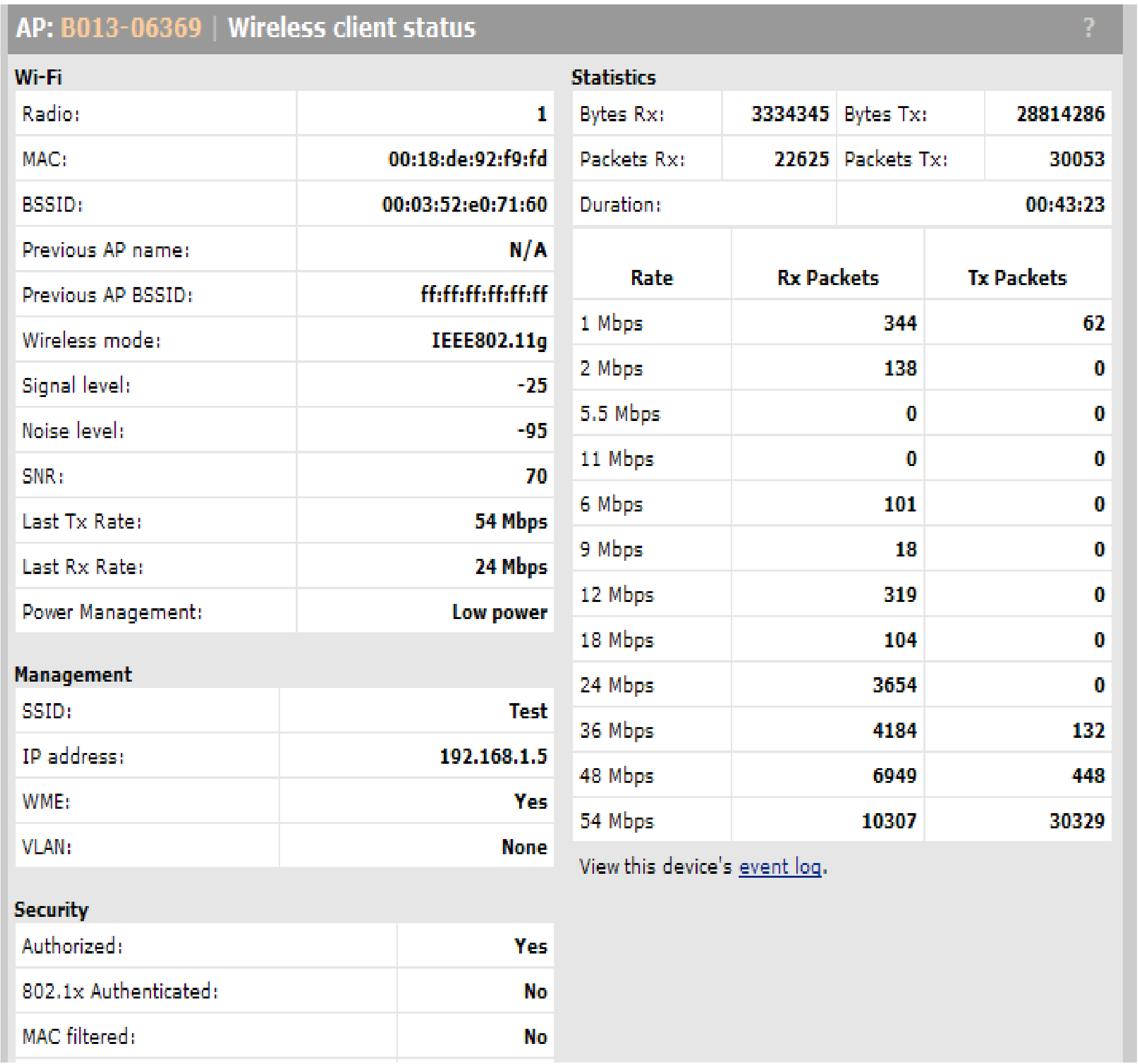
AP name	Radio	MAC address	IP address	SSID	Security	Duration	Signal	Noise	SNR

Figure 4-24: Wireless Clients

The **Wireless clients** page enables you to view the following information about each wireless user that is associated with the selected APs.

- **AP name**: Name of the AP the user is associated with.
- **Radio**: Radio on the AP that the user is using.
- **MAC Address**: MAC address of the user.
- **IP address**: IP address assigned to the user.
- **SSID**: The SSID though which the client connects.
- **Security**: Indicates if the user has been authorized.
- **Duration**: Indicates how long the user has been authorized.
- **SNR**: Indicates the relative strength of the user's radio signals versus the radio interference (noise) in the radio signal path. In most environments SNR is a good indicator for the quality of the radio link between the users and the AP. A higher SNR value means a better quality radio link.

You can select the MAC address link to display wireless client status details.



AP: B013-06369 | Wireless client status

Wi-Fi

Radio:	1
MAC:	00:18:de:92:f9:fd
BSSID:	00:03:52:e0:71:60
Previous AP name:	N/A
Previous AP BSSID:	ff:ff:ff:ff:ff:ff
Wireless mode:	IEEE802.11g
Signal level:	-25
Noise level:	-95
SNR:	70
Last Tx Rate:	54 Mbps
Last Rx Rate:	24 Mbps
Power Management:	Low power

Management

SSID:	Test
IP address:	192.168.1.5
WME:	Yes
VLAN:	None

Security

Authorized:	Yes
802.1x Authenticated:	No
MAC filtered:	No

Statistics

Bytes Rx:	3334345	Bytes Tx:	28814286
Packets Rx:	22625	Packets Tx:	30053
Duration:			00:43:23

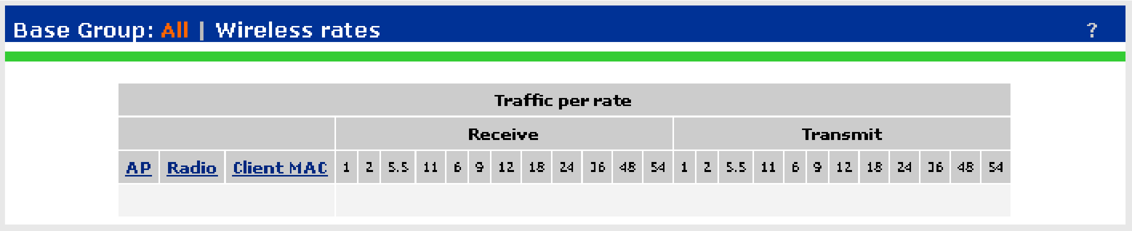
Rate	Rx Packets	Tx Packets
1 Mbps	344	62
2 Mbps	138	0
5.5 Mbps	0	0
11 Mbps	0	0
6 Mbps	101	0
9 Mbps	18	0
12 Mbps	319	0
18 Mbps	104	0
24 Mbps	3654	0
36 Mbps	4184	132
48 Mbps	6949	448
54 Mbps	10307	30329

View this device's event log.

Figure 4-25: Wireless Client Status Window

4.10.4 Wireless Rates

You can view information about the volume of traffic that has been sent and received at each data rate for wireless clients. In the Network tree, select **Controlled APs**, a group name, or an AP and then in the right pane select **Overview** > **Wireless rates**.



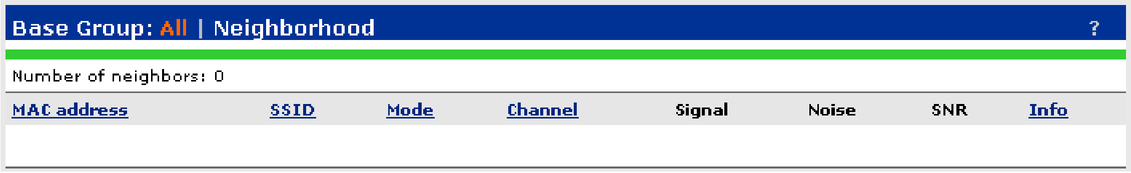
Base Group: All | Wireless rates ?

Traffic per rate																										
			Receive												Transmit											
AP	Radio	Client MAC	1	2	5.5	11	6	9	12	18	24	36	48	54	1	2	5.5	11	6	9	12	18	24	36	48	54

Figure 4-26: Wireless Rates

4.10.5 Neighborhood

You can view a list of all APs that are operating nearby to a specific controlled AP, all controlled APs, or a specific group of controlled APs by selecting in the right pane **Overview > Neighborhood.**



Base Group: All | Neighborhood ?

Number of neighbors: 0

MAC address	SSID	Mode	Channel	Signal	Noise	SNR	Info

Figure 4-27: Neighborhood

The list includes controlled APs, autonomous APs, and third-party APs and includes the following information about each:

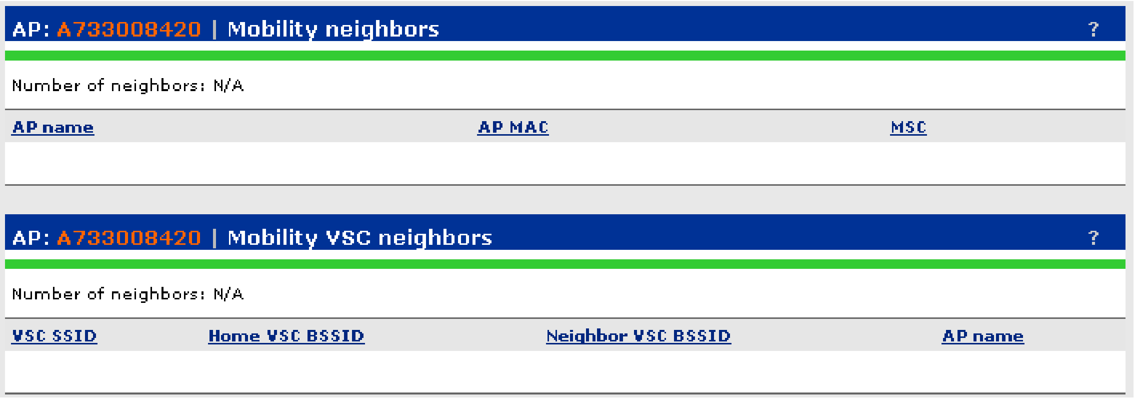
- **MAC address**: MAC address of the AP.
- **SSID**: SSID assigned to the AP.
- **Mode**: Indicates the operating mode of the AP: A, B, or G.
- **Channel**: Channel the AP is operating on.
- **Signal**: Signal strength.
- **Noise**: Amount of noise.
- **SNR**: Signal to noise ratio.
- **Info**: Additional information about the AP, such as the following:

- **WPA**: (or **WEP**, etc.) Some type of security is enabled on the AP.
- **ESS**: Operating in AP mode. Also lists security being used if enabled (WEP, WPA).
- **IBSS**: Operating in Ad-Hoc mode.

4.10.6 Mobility Neighbors

(Applies only to individual APs with the Mobility license.)

For a specific controlled + only, you can view a list of all APs that are in that AP's mobility neighborhood, as well as all virtual networks that are in the AP's mobility neighborhood, by selecting in the right pane **Overview** > **Mobility neighbors.**



AP: A733008420 | Mobility neighbors ?

Number of neighbors: N/A

AP name	AP MAC	MSC

AP: A733008420 | Mobility VSC neighbors ?

Number of neighbors: N/A

VSC SSID	Home VSC BSSID	Neighbor VSC BSSID	AP name

Figure 4-28: Mobility Neighbors

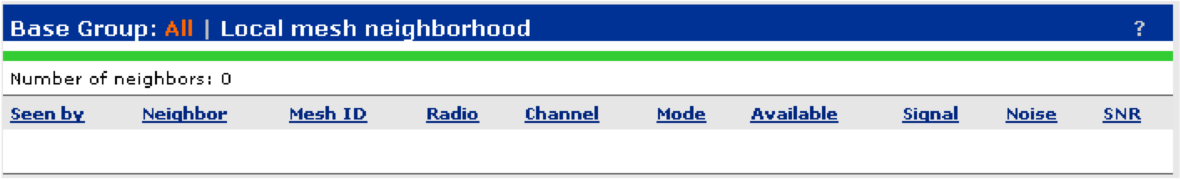
Information is provided as follows:

- **Mobility neighbors**
  - **AP name**: Name of the AP.
  - **AP MAC**: AP's MAC address.
  - **Controller**: Name of service controller that controls the AP.
- **Mobility virtual network neighbors**
  - **virtual network**: virtual network name.
  - **SSID**: SSID associated with the virtual network.

- **Home VSC BSSID**: BSSID of the home virtual network.
- **Neighbor VSC BSSID**: BSSID of the neighboring virtual network.
- **AP name**: Name of the AP that the neighboring virtual network is defined on.

4.10.7 Local Mesh Neighborhood

This page lists all APs that have active local mesh nodes.



Base Group: All | Local mesh neighborhood ?

Number of neighbors: 0

Seen by	Neighbor	Mesh ID	Radio	Channel	Mode	Available	Signal	Noise	SNR

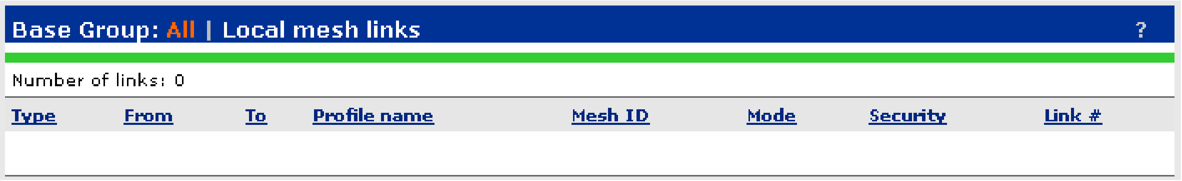
Figure 4-29: Local Mesh Neighborhood

Information is provided as follows:

- **Seen by**: Name of AP that discovered the node.
- **Neighbor**: Name or MAC address of the neighboring node.
- **Mesh ID**: Indicates the mesh ID of the node. Mesh IDs are unique numbers that are used to identify a series of nodes that can connect together to form a local mesh.
- **Radio**: Radio being used by the node.
- **Channel**: Channel being used by the node.
- **Mode**: Indicates if the node is operating as a master, slave, or alternate master.
- **Available**: Indicates if the node is available to establish a link.
- **SNR**: Indicates the relative strength of the remote's radio signals versus the radio interference (noise) in the radio signal path. In most environments, SNR is a good indicator for the quality of the radio link between the local and remote nodes. A higher SNR value means a better quality radio link.

4.10.8 Local Mesh Links

This page lists all local mesh links.



Base Group: All | Local mesh links ?

Number of links: 0

Type	From	To	Profile name	Mesh ID	Mode	Security	Link #

Figure 4-30: Local Mesh Links

Information is provided as follows:

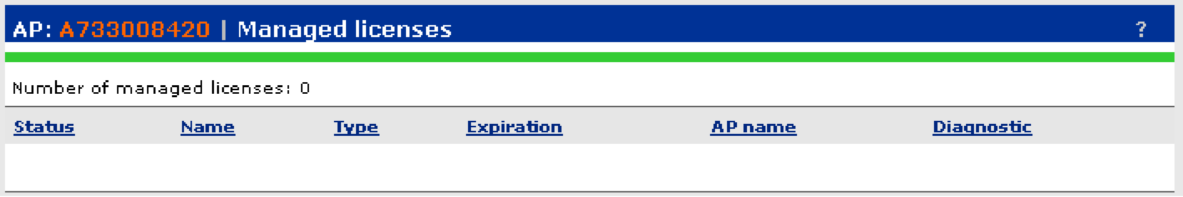
- **Type**: Type of link: master or slave.
- **From**: Name of AP that originated the link.
- **To**: Name of AP that accepted the link.
- **Profile name**: Name assigned to the profile.
- **Mesh ID**: Indicates the mesh ID of the node. Mesh IDs are unique numbers that are used to identify a series of nodes that can connect together to form a local mesh.
- **Mode**: Indicates if the node is operating as a master, slave, or alternate master.
- **Security**: Indicates the type of security that is enabled.
- **Link #**: A master may have multiple links to slave nodes. Each link is assigned a different number for identification purposes.

4.10.9 Licenses

For information about licenses installed on the service controller for distribution to APs.

You can view a list of all managed licenses on a specific controlled AP, all controlled APs, or a specific group of controlled APs by selecting **Overview > Licenses**.

Information is provided as follows:



AP: A733008420 | Managed licenses

Number of managed licenses: 0

Status	Name	Type	Expiration	AP name	Diagnostic

Figure 4-31: Managed Licenses

- **Status**: Indicates if the license is active or not.
- **Name**: Identifies the license.
- **Type**: License type either permanent or temporary.
- **Expiration**: Indicates the expiry date for the license.
- **AP name**: Name of the AP that the license is associated with.

Diagnostic: Provides diagnostic information for licenses that are not active.

5

Chapter 5 - Working with Virtual Networks

In This Chapter:

5.1 Key Concepts

A VSC (virtual service community) is a collection of configuration settings that define key operating characteristics of the service controller and controlled APs. In most cases, a virtual network is used to define the characteristics of a wireless network.

A service controller supports up to sixteen virtual network profiles, allowing for great flexibility in the configuration of services. For example, in the following scenario four virtual networks are used to support different types of wireless users. Each virtual network is configured with a different wireless network name (SSID), and the quality of service (QoS) feature is used to classify user traffic priority.

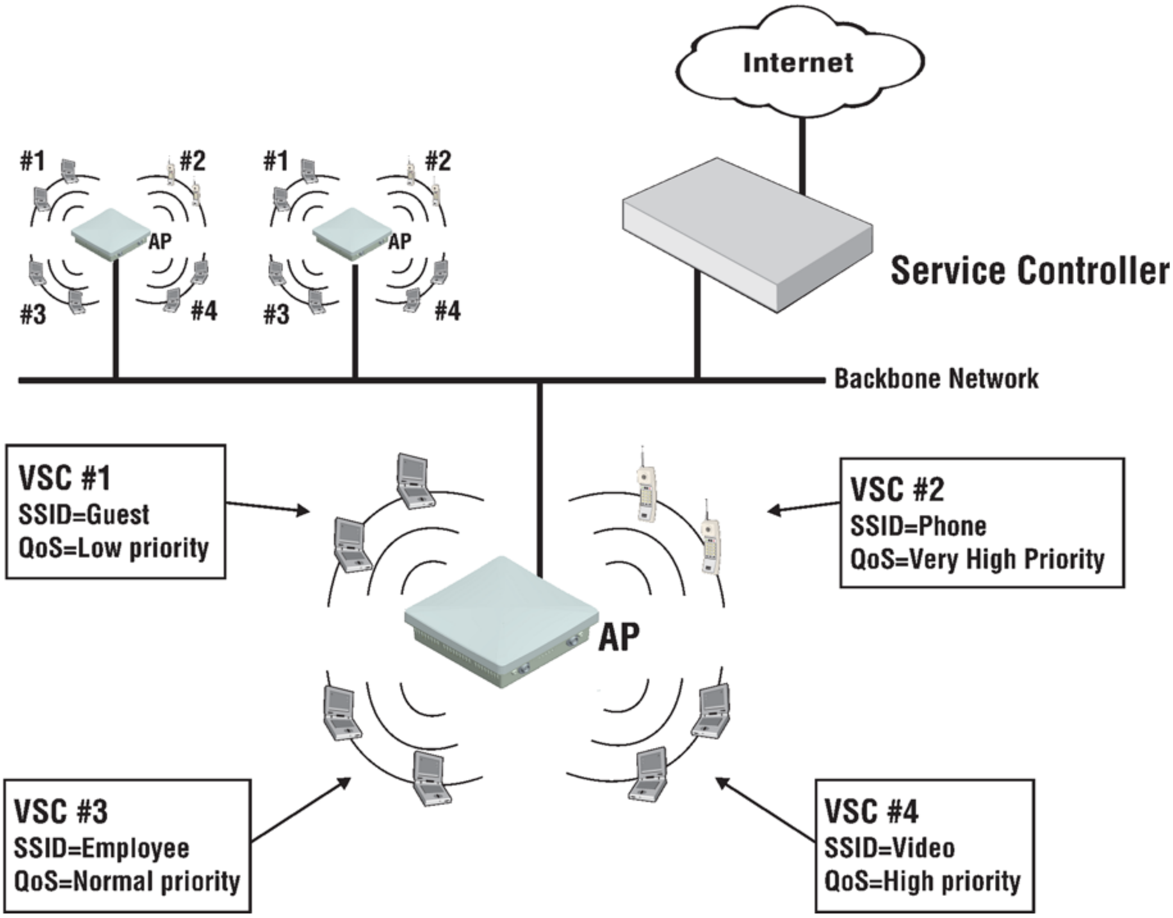


Figure 5-1: VSCs

The service controller defines a global pool of virtual networks that represents the services that are available on the network. From this pool, specific virtual networks can be *bound* to one or more groups (and the APs in the groups), to provide a homogeneous wireless offering. (See binding “Binding Virtual Networks to Groups” on page 64)

See one of my previous comment. We should explain that what you define here is a pool of virtual network (up to 16) that can be thereafter referenced/distributed in the network and the APs through the bindings. However, an important point is that Access Controlled virtual networks also apply at the service controller to handle public access user traffic. Another note on the particularity of the 1st virtual network must be delivered. This is a default virtual network that has a special meaning in the system. It is used as a fallback for any traffic that goes through the service controller and that cannot be identified as coming from a Alvarion AP or with a VLAN ID information (i.e. traffic from 3rd-party APs or wired stations on the network if no VLAN ID is assigned).

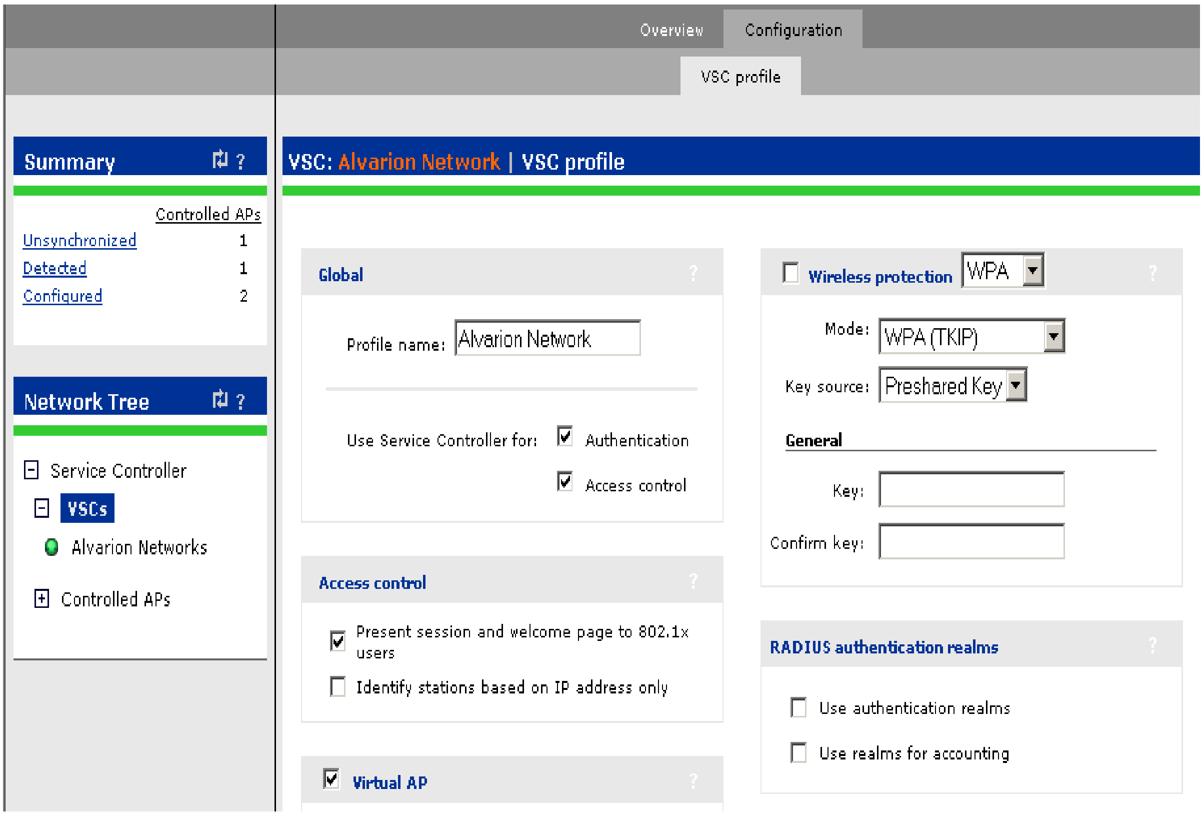
5.1.1 Virtual Network Configuration Examples

The *Deployment Guide* provides numerous detailed examples on virtual network configuration when using the service controller with both controlled and autonomous APs.

5.1.2 Virtual Network List

This section provides a summary of all configurable virtual network features. The screen images in this section are taken from the virtual network profile page which opens when you are adding or editing a virtual network definition.

To add a virtual network, select V**irtual networks >> Overview > Add New virtual network Profile**.



VSC: Alvarion Network | VSC profile

Controlled APs	
Unsynchronized	1
Detected	1
Configured	2

Service Controller
VSCs
Alvarion Networks
Controlled APs

Global

Profile name: Alvarion Network

Use Service Controller for: ☑ Authentication ☑ Access control

Access control

☑ Present session and welcome page to 802.1x users

□ Identify stations based on IP address only

☑ **Virtual AP**

□ **Wireless protection** WPA

Mode: WPA (TKIP)

Key source: Preshared Key

General

Key:

Confirm key:

RADIUS authentication realms

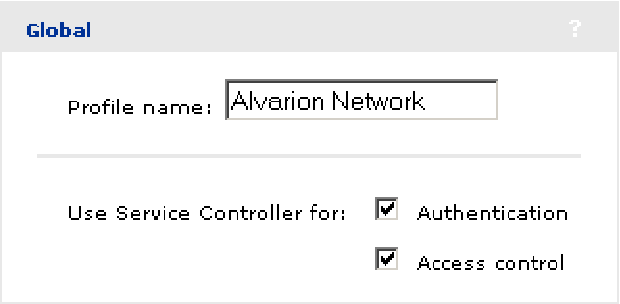
□ Use authentication realms

□ Use realms for accounting

Figure 5-2: Adding a Virtual Network

5.1.3 About Access Control And Authentication

Availability of certain virtual network features and their functionality are dependent on the setting of two important parameters in the virtual network's **Global** box. These parameters determine how authentication and access control are handled by the virtual network:



Global

Profile name: Alvarion Network

Use Service Controller for: ☑ Authentication ☑ Access control

Figure 5-3: Access Control and Authentication

- **Use Service Controller for: Authentication:** Determines if user authentication services (802.1X, WPA, WPA2) are provided by the service controller. When enabled, APs forward user login requests to the service controller. The service controller resolves these requests using the local user accounts, Active Directory, or acts as a RADIUS proxy for a third-party RADIUS server.

- **Use service controller for: Access control:** This option can only be enabled if the **Authentication** is enabled first. When enabled, controlled APs forward authenticated user traffic to the service controller, which manages access to the protected network.

NOTE

When access control is disabled, the virtual network can only be used to handle wireless traffic on a controlled AP.

The following diagrams provide an overview of how user authentication and data traffic are handled depending on how these options are configured

5.1.3.1 Both Authentication and Access Control are Enabled

In this configuration, the controlled AP forwards authentication requests to the service controller. The service controller resolves these requests using the local user list, or uses the services of a third-party authentication server (Active Directory or RADIUS server). The service controller then manages user access to the protected network.

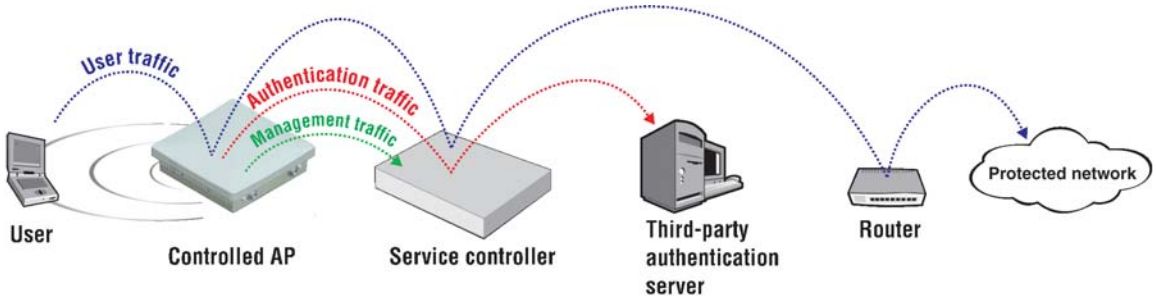


Figure 5-4: [Authentication and Access Control Enabled]

5.1.3.2 Only Authentication is Enabled

In this configuration, the controlled AP forwards authentication requests to the service controller. The service controller resolves these requests using the local user list, or uses the services of a third-party authentication server (Active Directory or RADIUS server).

The controlled AP forwards all authenticated user traffic to the protected network (or another device performing access control) according to settings defined on the controlled AP.

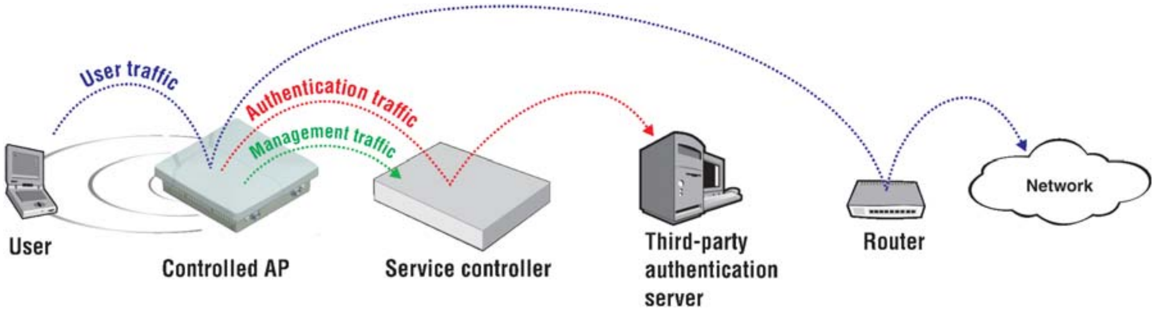


Figure 5-5: [Only Authentication is Enabled]

5.1.3.3 Neither Option is Enabled

In this configuration, the controlled AP resolves authentication requests using a third-party RADIUS server and forwards authenticated user traffic to the protected network (or another device performing access control). In this scenario, the service controller is used for management of the AP only.

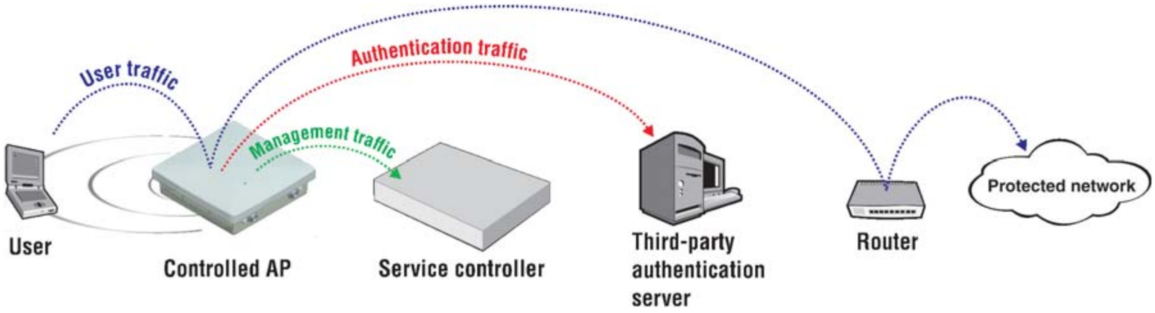


Figure 5-6: [Neither Authentication Nor Access Control are Enabled]

5.1.4 Centralized Access Control

This feature enables controlled APs to create a data tunnel to the service controller to transport all user traffic, providing the following benefits:

- User traffic is segregated from the backbone network and can only travel to the service controller.

- Underlying network topology is abstracted enabling full support for L2-connected users across routed networks.
- Enables discovery to be performed on Internet port.

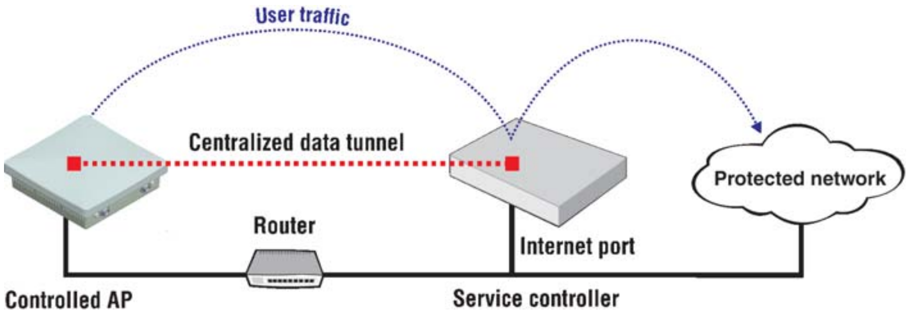
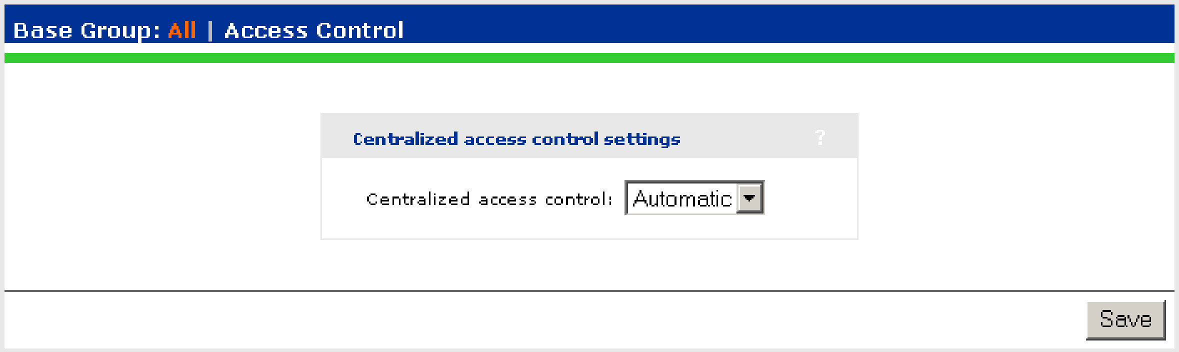


Figure 5-7: Centralized Access Control

To enable this option, select **Controlled APs** >> **Configuration** > **Access control**. (You can also set this at the group or AP level).


Base Group: All | Access Control
Centralized access control settings
Save

Centralized access control: Automatic

Figure 5-8: Centralized Access Control: Automatic

Select one of the following options to specify how the tunnel will be created:

- **Automatic**: A tunnel is created only if a router is detected between the AP and the service controller. This is the default option.
- **Enabled**: A tunnel is always created between the AP and the service controller.
- **Disabled**: No tunnel is created.

NOTE

This feature is not supported if the connection between the AP and service controller traverses a network device that provides network address translation (NAT)

5.2 Virtual Network Configuration Options

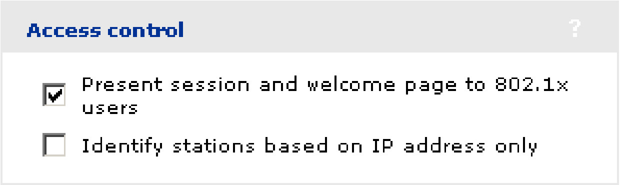
The following table lists the virtual network configuration options that are available depending on how access control and authentication are configured.

VSC configuration option	Use service controller for:		
	Authentication and Access control	Authentication only	Neither
Access control	X		
Virtual AP	X	X	X
VSC ingress mapping	X		
VSC egress mapping	X		
Default user data rates	X		
Wireless mobility		X	X
Wireless security filters	X	X	X
Wireless protection	X	X	X
RADIUS authentication realms	X	X	
HTML-based user logins	X		
MAC-based authentication	X	X	X
Location-aware	X		
Wireless MAC filter	X	X	X
Wireless IP filter	X	X	X
DHCP server	X		
DHCP relay	X		

This sections that follow provide an overview of each virtual network option and how it can be used. For complete descriptions of individual parameters refer to the online help in the management tool.

5.2.1 Access Control

These settings determine if 802.1X users will see the public access interface Session page after they login.



Access control

☑ Present session and welcome page to 802.1x users

□ Identify stations based on IP address only

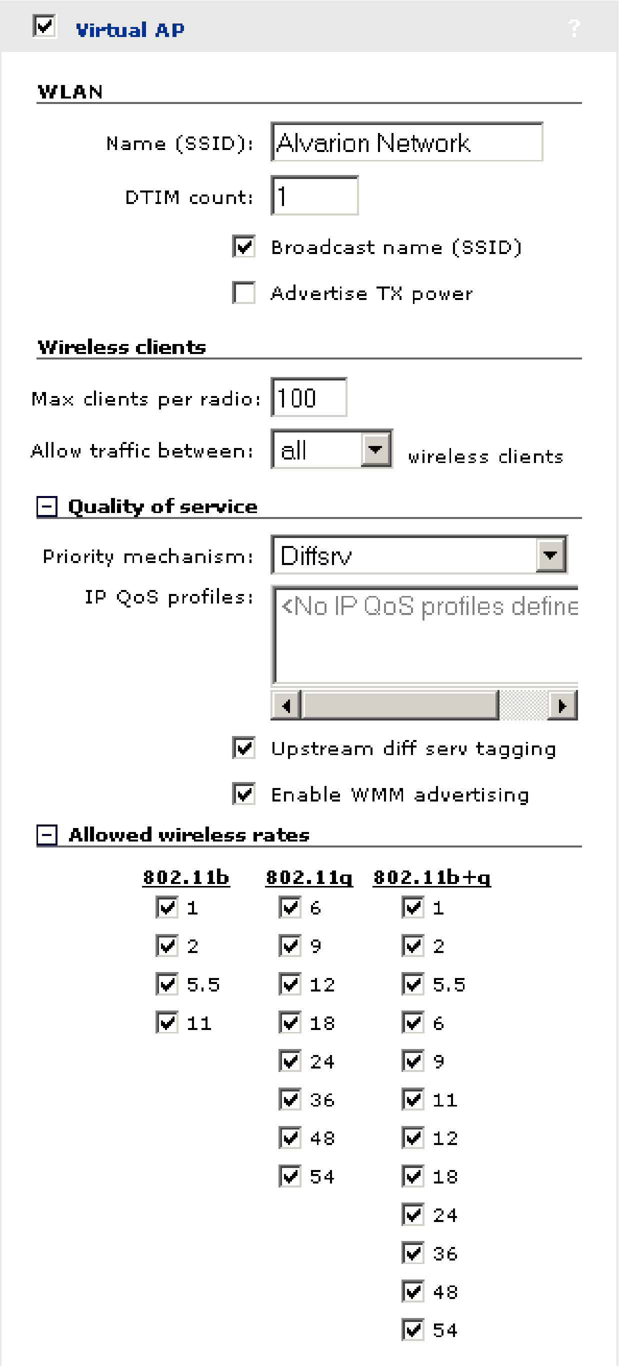
Figure 5-9: Access Control

NOTE

Display of the Session page may not work for all users. It will fail if the initial traffic from the user's computer is sent by an application other than the user's browser. For example: messaging software, automatic software update services, email applications.

5.2.2 Virtual AP

These settings define the characteristics of the wireless network created by the virtual network, including its name, the number of clients supported, and quality of service settings.



☑ Virtual AP

WLAN

Name (SSID): Alvarion Network

DTIM count: 1

☑ Broadcast name (SSID)

□ Advertise TX power

Wireless clients

Max clients per radio: 100

Allow traffic between: all wireless clients

⊟ Quality of service

Priority mechanism: Diffsrv

IP QoS profiles: <No IP QoS profiles define

☑ Upstream diff serv tagging

☑ Enable WMM advertising

⊟ Allowed wireless rates

802.11b	802.11g	802.11b+g
☑ 1	☑ 6	☑ 1
☑ 2	☑ 9	☑ 2
☑ 5.5	☑ 12	☑ 5.5
☑ 11	☑ 18	☑ 6
	☑ 24	☑ 9
	☑ 36	☑ 11
	☑ 48	☑ 12
	☑ 54	☑ 18
		☑ 24
		☑ 36
		☑ 48
		☑ 54

Figure 5-10: Virtual AP

5.2.2.1 Quality of Service

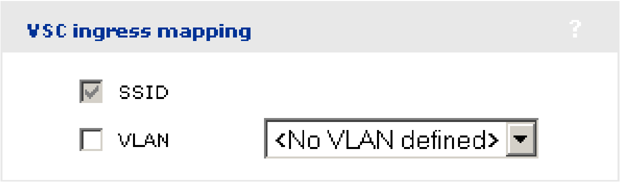
Lets you prioritize traffic on the virtual network. See for "Quality of Service (QoS)" on page 127 details.

5.2.2.2 Allowed Wireless Rates

Lets you select the wireless transmission speeds that are supported for each wireless mode.

5.2.3 VSC Ingress Mapping

These settings apply to the service controller only and define how ingress traffic on the LAN port is assigned to a virtual network. For details refer to “Virtual Network Data Flow” on page 120.



VSC ingress mapping

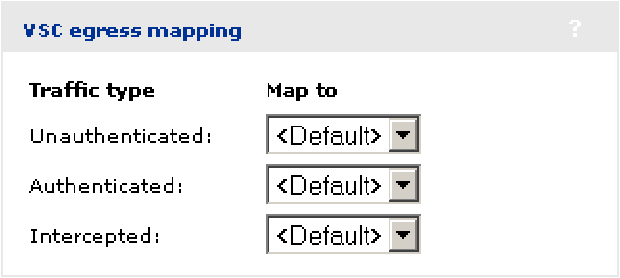
☑ SSID

□ VLAN <No VLAN defined>

Figure 5-11: VSC Ingress Mapping

5.2.4 VSC Egress Mapping

These options select the service controller’s output interface on which a virtual network forwards user traffic. (To set virtual network egress options for controlled APs, see “Binding a Virtual Network to a Group” on page 67.) Different types of traffic can be forwarded to different output interfaces, which include the routing table, VLAN ID, or an IP GRE tunnel. Before you can map traffic to an output interface, the interface must already be defined. For details refer to “Virtual Network Data Flow” on page 120.



VSC egress mapping

Traffic type	Map to
Unauthenticated:	<Default>
Authenticated:	<Default>
Intercepted:	<Default>

Figure 5-12: VSC Egress Mapping

In the above example, with all defaults selected, the service controller routing table is used for all egress traffic. Therefore, all ingress traffic on this virtual network is routed according to the routes defined on the **Service Controller** >> **Network** > **IP routes** page.

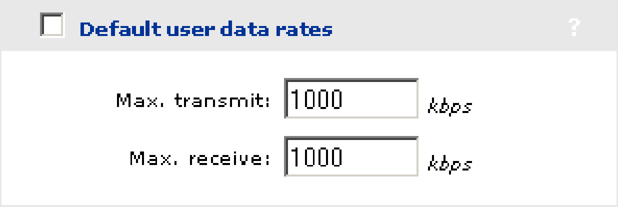
NOTE

Traffic from specific users can be **Intercepted**. To enable traffic interception for a specific user, you must specify the appropriate setting in the user's RADIUS account. See the *Network Access Admin Guide for* details.

5.2.5 Default User Data Rates

These options enable you to set the default data rates for authenticated users that do not have a data rate set in their RADIUS accounts and unauthenticated users. See the *Network Access Admin Guide* for details on setting the appropriate RADIUS attributes to accomplish this.

The throughput limits globally defined on the **Service Controller** >> **Network** > **Bandwidth control** page always take precedence over user data rates. This means if you set a data rate which exceeds the configured bandwidth level, the rate will be capped at the bandwidth level.



□ Default user data rates

Max. transmit: 1000 kbps

Max. receive: 1000 kbps

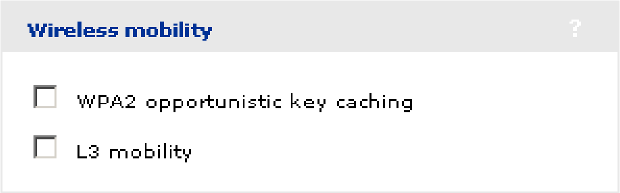
Figure 5-13: Default User Data Rates

5.2.6 Wireless Mobility

Mobility services are only available when **Access control** is disabled (under **General**) and the appropriate license is installed.

- WPA2 opportunistic key caching eliminates the delays associated with reauthentication when users roam between APs on the same layer 2 network. This also requires that WPA2 be used.

- Layer 3 mobility enables users to move between APs that are connected to different IP subnets while maintaining their assigned IP address. Typical applications are VoWLAN and the roaming and maintaining of VoWLAN calls when moving between subnets.



Wireless mobility

□ WPA2 opportunistic key caching

□ L3 mobility

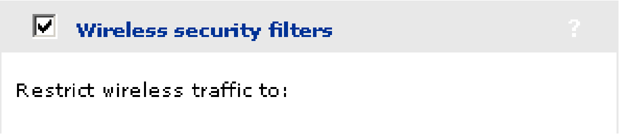
Figure 5-14: Wireless Mobility

For more information, see Wireless Mobility.

5.2.7 Wireless Security Filters

APs feature an intelligent bridge that can apply security filters to safeguard the flow of wireless traffic. These filters limit both incoming and outgoing traffic as defined below and force the APs to exchange traffic with a specific upstream device.

- If **Access control** is enabled (under **General**), the controlled AP will only allow user traffic that is addressed to the service controller. All other traffic is blocked. Make sure that the service controller is set as the default gateway for all users. If not, all user traffic will be blocked by the AP.

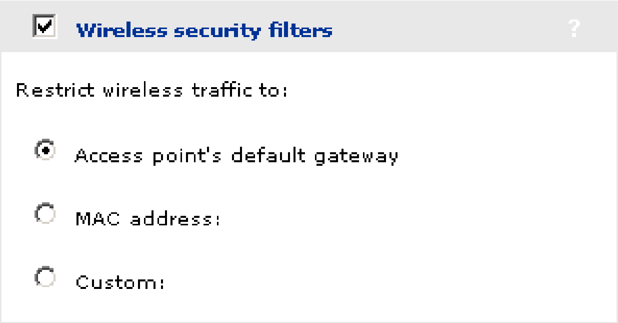


☑ Wireless security filters

Restrict wireless traffic to:

Figure 5-15: Wireless Security Filters when Access Control is Enabled

- If **Access control** is disabled (under **General**), then the security filters can be used to block traffic unless it is addressed to a specific device.



☑ Wireless security filters

Restrict wireless traffic to:

● Access point's default gateway

○ MAC address:

○ Custom:

Figure 5-16: Wireless Security Filters when Access Control is Disabled

Use the **Custom** option to define a custom filter with standard pcap syntax and a few Alvarion-specific placeholders. See the online help for details.

5.2.8 Wireless Protection

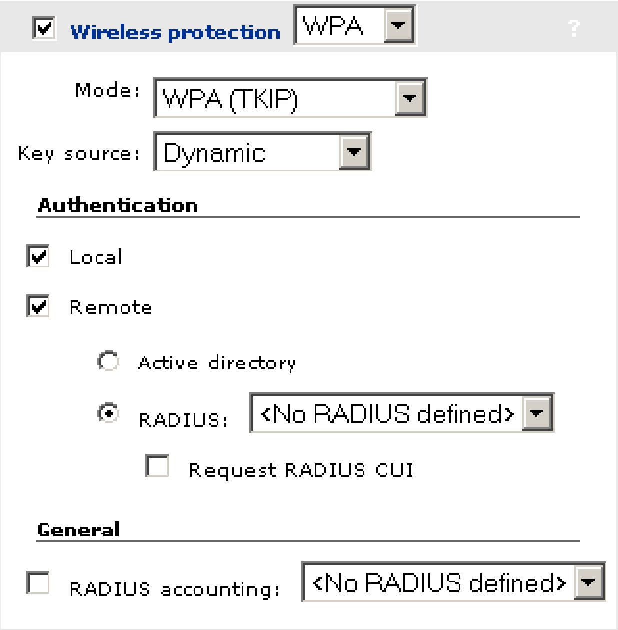
Three types of wireless protection are offered.

5.2.8.1 WPA

This option enables support for users with WPA / WPA2 client software. Support is provided for

- **WPA (TKIP)**: WPA with TKIP encryption.
- **WPA2 (AES/CCMP)**: WPA2 (802.11i) with CCMP encryption.
- **WPA or WPA2**: Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time.

Authentication can occur via the local user accounts and remote authentication server (Active Directory, or third-party RADIUS server). If both options are enabled, the local accounts are checked first.



☑ Wireless protection: WPA

Mode: WPA (TKIP)

Key source: Dynamic

Authentication

☑ Local

☑ Remote

○ Active directory

● RADIUS: <No RADIUS defined>

□ Request RADIUS CUI

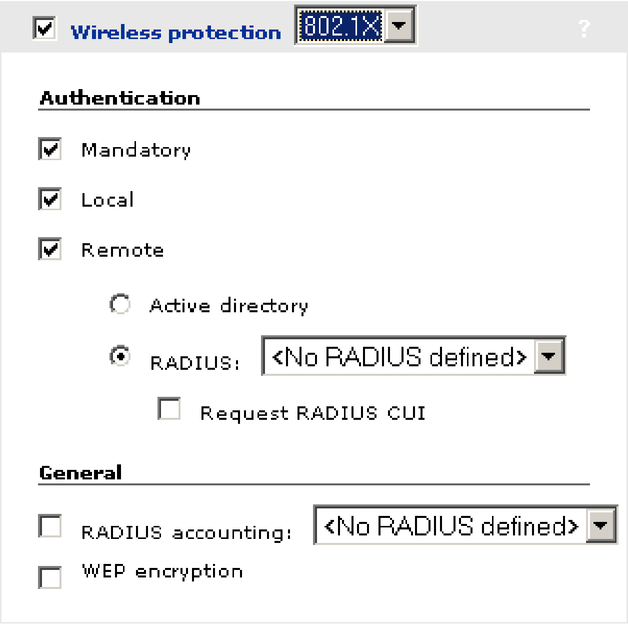
General

□ RADIUS accounting: <No RADIUS defined>

Figure 5-17: WPA

5.2.8.2 802.1X

This option enables support for users with 802.1X client software that use any of the following authentication methods: EAP-TLS, EAP-TTLS, and EAP-PEAP. Additionally, when an external RADIUS server is used, support for EAP-SIM, EAP-AKA, EAP-FAST, and EAP-GTC is also provided. Check your external RADIUS server for supported authentication methods.



☑ Wireless protection 802.1X

Authentication

☑ Mandatory

☑ Local

☑ Remote

○ Active directory

● RADIUS: <No RADIUS defined>

□ Request RADIUS CUI

General

□ RADIUS accounting: <No RADIUS defined>

□ WEP encryption

Figure 5-18: 802.1X

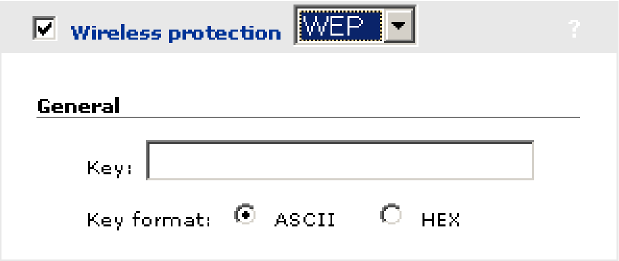
NOTE

If 802.1X is used without enabling WEP, wireless traffic will be unencrypted.

When the **Mandatory** option is enabled, all users must authenticate using 802.1X, regardless of whether other methods are active, before they can gain access to the egress interface.

5.2.8.3 WEP

This option provides support for users using WEP encryption.



☑ Wireless protection WEP

General

Key:

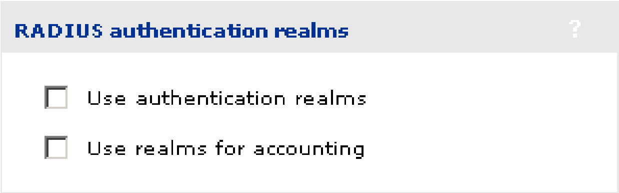
Key format: ● ASCII ○ HEX

Figure 5-19: WEP

5.2.9 RADIUS Authentication Realms

When realms are enabled for accounting or authentication, selection of the RADIUS server to use is based on the realm name. If no match is found, then the configured RADIUS profile name is used.

This applies to any virtual network authentication or accounting setting that uses a RADIUS server.



RADIUS authentication realms

□ Use authentication realms

□ Use realms for accounting

Figure 5-20: Radius Authentication Realms

NOTE

The virtual network-defined RADIUS server becomes the default when no servers based on the realm are detected.

Realm names are extracted from user names as follows: if the username is **person1@mydomain.com** then **mydomain.com** is the realm. The authentication request is sent to the RADIUS profile with the realm name **mydomain.com**. The username sent for authentication is still the complete **person1@mydomain.com**.

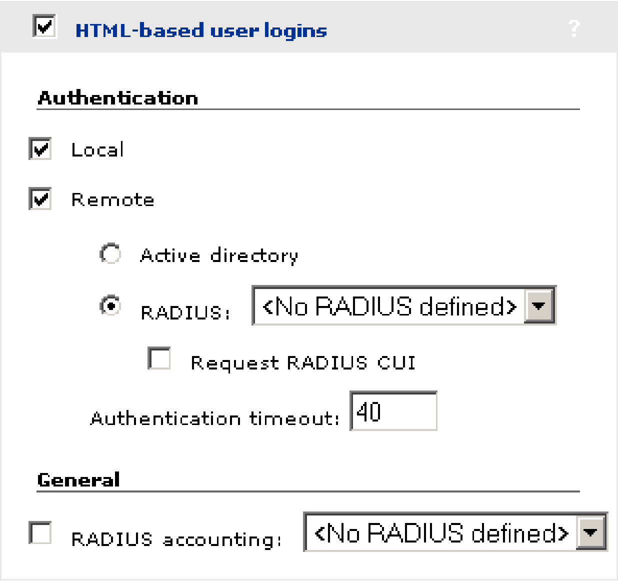
For added flexibility, regular expressions can be used in realm names, enabling a single realm name to match many users. For example, if a realm name is defined with the regular expression **^per.*** then all usernames beginning with **per** followed by any number of characters will match. The following usernames would all match:

per123.biz
per321.lan
per1

5.2.10 HTML-based User Logins

This option defines settings for users who log in to the public access interface using a web browser. If you disable this option, the public access interface Login page is not shown to these users. However, login is still possible via other methods such as MAC authentication and 802.1X.

Authentication can occur via the local user accounts and a remote server (Active Directory or RADIUS). If both options are enabled, the local user accounts are always checked first.



☑ HTML-based user logins

Authentication

☑ Local

☑ Remote

○ Active directory

● RADIUS: <No RADIUS defined>

□ Request RADIUS CUI

Authentication timeout: 40

General

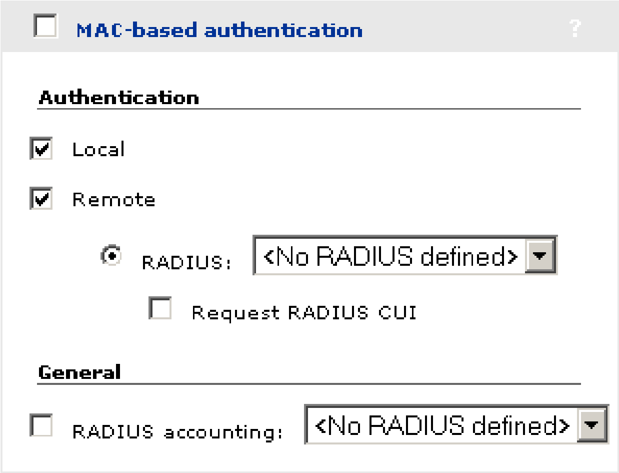
□ RADIUS accounting: <No RADIUS defined>

Figure 5-21: HTML-based User Logins

5.2.11 MAC-based Authentication

This option can only be used to authenticate wireless users. If used on a virtual network that supports both wired and wireless users, wired users gain access without having to authenticate.

This option enables wireless users to be authenticated by their MAC addresses. Authentication can occur via the local user accounts and a remote RADIUS server. If both options are enabled, the local user accounts are checked first.



□ MAC-based authentication

Authentication

☑ Local

☑ Remote

● RADIUS: <No RADIUS defined>

□ Request RADIUS CUI

General

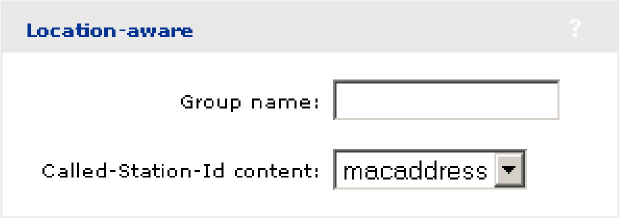
□ RADIUS accounting: <No RADIUS defined>

Figure 5-22: MAC-based Authentication

5.2.12 Location-aware

This option enables you to control logins to the public access network based on the AP, or group of APs, to which a user is connected. It is automatically enabled when a virtual network is set to **Access control**. Location-aware is always enabled when using the service controller for authentication or access-control with a remote RADIUS server.

For each user login, location-aware sends the PHY Type, SSID, and VLAN to the remote RADIUS server. It also includes the specified **Called-Station-Id content.**



Location-aware

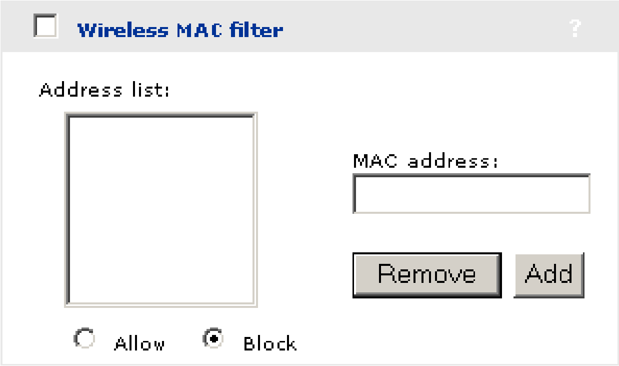
Group name:

Called-Station-Id content: macaddress

Figure 5-23: Location-aware

5.2.13 Wireless MAC Filter

This option enables you to control access to the wireless network based on the MAC address of device. You can either block access or allow access, depending on your requirements.



□ Wireless MAC filter

Address list:

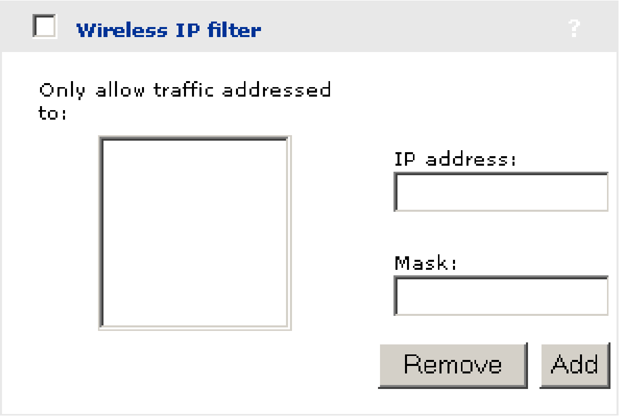
MAC address:

○ Allow ● Block

Figure 5-24: Wireless MAC Filter

5.2.14 Wireless IP Filter

This option enables you to only allow wireless-to-wired LAN traffic for specific destination addresses.



□ Wireless IP filter

Only allow traffic addressed to:

IP address:

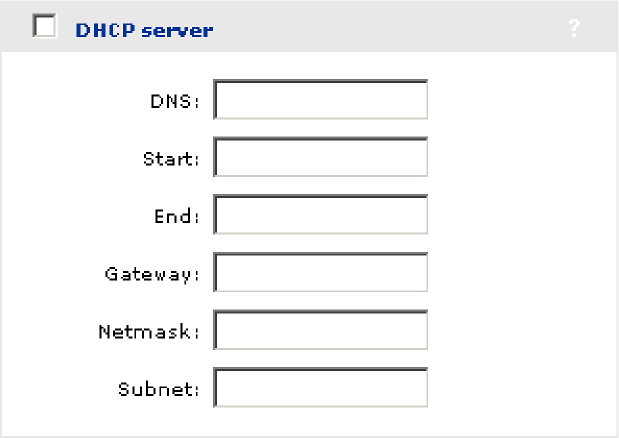
Mask:

Figure 5-25: Wireless IP Filter

5.2.15 DHCP Server

This option is only available if the service controller is currently configured as a DHCP server on the **Service Controller** >> **Network** > **Address allocation** page (“Address Allocation” on page 157).

A separate DHCP server can be enabled on each virtual network to provide custom addressing to users. This enables you to assign different IP address ranges for each virtual network. In order to receive traffic from users, the service controller assigns the **Gateway** address you specify to its LAN port.



□ DHCP server

DNS:

Start:

End:

Gateway:

Netmask:

Subnet:

Figure 5-26: DHCP Sever

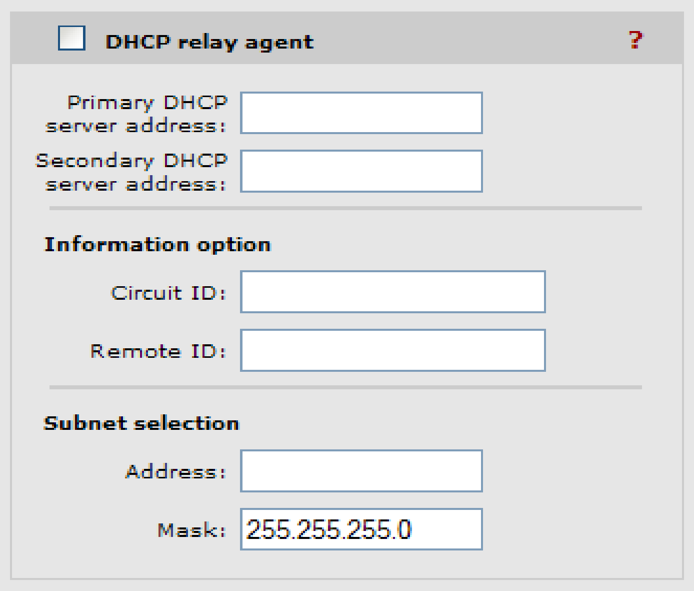
NOTE

These configuration options do not appear for the default virtual network. The default virtual network uses the same settings as defined on the **Service Controller >> Network > Address allocation** page ("Address Allocation" on page 157).

5.2.16 DHCP Relay Agent

This option is only available if the service controller is currently configured as a DHCP relay agent on the **Service Controller** >> **Network** > **Address allocation** page ("Address Allocation" on page 157).

A separate DHCP relay agent can be enabled on each virtual network to provide custom addressing to users.



☐ DHCP relay agent ?

Primary DHCP server address:

Secondary DHCP server address:

Information option

Circuit ID:

Remote ID:

Subnet selection

Address:

Mask: 255.255.255.0

Figure 5-27: DHCP Relay Agent[

NOTE

These configuration options do not appear for the default virtual network. The default virtual network uses the same settings as defined on the **Service Controller >> Network > Address allocation** page (“Address Allocation” on page 157).

5.3 Virtual Network Data Flow

Each virtual network provides a number of configurable options, some of which apply exclusively on controlled APs or the service controller. The following diagrams illustrate how traffic from wireless users is handled by virtual network definitions on a controlled AP and service controller, and shows the options that apply on each device.

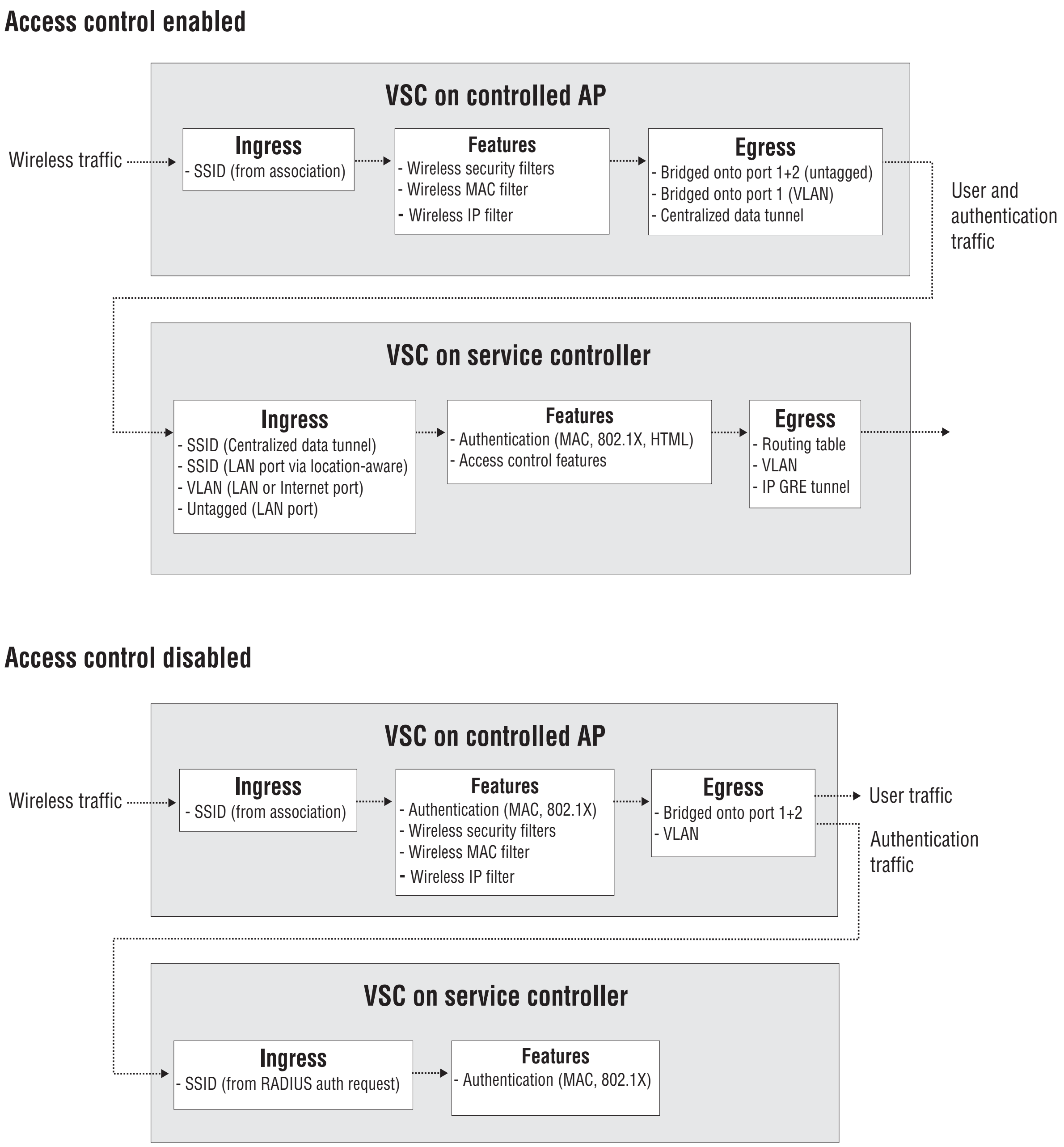

Access control enabled
VSC on controlled AP
Wireless traffic
Ingress
- SSID (from association)
Features
- Wireless security filters
- Wireless MAC filter
- Wireless IP filter
Egress
- Bridged onto port 1+2 (untagged)
- Bridged onto port 1 (VLAN)
- Centralized data tunnel
User and authentication traffic
VSC on service controller
Ingress
- SSID (Centralized data tunnel)
- SSID (LAN port via location-aware)
- VLAN (LAN or Internet port)
- Untagged (LAN port)
Features
- Authentication (MAC, 802.1X, HTML)
- Access control features
Egress
- Routing table
- VLAN
- IP GRE tunnel
Access control disabled
VSC on controlled AP
Wireless traffic
Ingress
- SSID (from association)
Features
- Authentication (MAC, 802.1X)
- Wireless security filters
- Wireless MAC filter
- Wireless IP filter
Egress
- Bridged onto port 1+2
- VLAN
User traffic
Authentication traffic
VSC on service controller
Ingress
- SSID (from RADIUS auth request)
Features
- Authentication (MAC, 802.1X)

Figure 5-28: Virtual Network Data Flow

5.3.1 Access Control Enabled

5.3.1.1 Virtual Network on Controlled AP

5.3.1.1.1 Ingress

The AP only handles wireless traffic. The SSID is the name of the wireless network that the user associates with.

5.3.1.1.2 Features

- **Wireless security filters:** Enables the AP to block traffic unless it is addressed to a specific destination (like the service controller). For more information, see “Wireless Security Filters” on page 110.
- **Wireless MAC filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses.
- **Wireless IP filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user IP addresses.

5.3.1.1.3 Egress

- **Bridged onto port 1+2 (untagged):** Untagged user and authentication traffic is bridged onto ports 1 and 2.
- **Bridged onto port 1 (VLAN):** VLAN tagged traffic is bridged onto port 1 only. VLAN tags can be assigned on a per-user basis via RADIUS attributes (“Defining Account Profiles” on page 270), or for all traffic on a virtual network (“Defining VLANs” on page 73).
- **Centralized data tunnel:** When this option is enabled, the AP creates a data tunnel to the service controller to carry all user traffic. For more information, see “Centralized Access Control” on page 102.

5.3.1.2 Virtual Network on Service Controller

5.3.1.2.1 Ingress

- **SSID (Centralized data tunnel):** When a centralized mode data tunnel has been created to the AP, all user traffic comes in on it. For more information, see “Centralized Access Control” on page 102. The tunnel is established to the same interface on which the AP was discovered. (LAN or Internet port).
- **SSID (LAN port):** SSID is retrieved using the location-ware function.
- **VLAN (LAN or Internet port):** Traffic with a VLAN ID is handled by the virtual network with a matching VLAN definition. See “Using Multiple Virtual Networks” on page 125 for more information.
- **Untagged (LAN port):** Untagged traffic on the LAN port may originate from wired users, or APs operating in autonomous mode (Alvarion or third-party).

5.3.1.2.2 Features

- **Authentication:** The service controller supports 802.1X, MAC, or HTML authentication. To validate user login credentials the service controller can use the local user accounts or make use of a third-party authentication server (Active Directory or RADIUS). For more information, see "Authentication Types" on page 261.

- **Access control features:** The service controller provides a number of features that can be applied to user sessions. Features can be enabled globally or on a per-account basis. For more information. For more information, see "Global Access Control Settings" on page 280 and "Account Profiles" on page 267.

5.3.1.2.3 Egress

The service controller enables user traffic to be forwarded to different output interfaces, which include the routing table, VLAN ID, or GRE tunnel. For more information, see "VSC Egress Mapping" on page 108.

5.3.2 Access Control Disabled

5.3.2.1 Virtual Network on Controlled AP

5.3.2.1.1 Ingress

The AP only handles wireless traffic. The SSID is the name of the wireless network that the user associates with.

5.3.2.1.2 Features

- **Authentication:** The AP supports 802.1X or MAC authentication. To validate user login credentials the AP makes use of a third-party authentication server (service controller or third-party RADIUS server). For more information, see "Authentication Types" on page 261.

- **Wireless security filters:** Enables the AP to block traffic unless it is addressed to a specific destination (like the service controller). For more information, see "Wireless Security Filters" on page 110.

- **Wireless MAC filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses.

- **Wireless IP filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user IP addresses.

5.3.2.1.3 Egress

- **Bridged onto port 1+2:** Unless a centralized mode tunnel has been established, user and authentication traffic is bridged onto ports 1 and 2.
- **VLAN:** VLAN tags can be assigned for all traffic on a virtual network. For more information, see "Defining VLANs" on page 73.

5.3.2.2 Virtual Network on Service Controller

5.3.2.2.1 Ingress

- **SSID (from RADIUS auth request):** The service controller determines the SSID from the RADIUS authentication request sent by the AP, and uses this SSID to determine the virtual network to use for authentication.

5.3.2.2.2 Features

- **Authentication:** The service controller supports 802.1X or MAC authentication. To validate user login credentials the service controller can use the local user accounts or make use of a third-party authentication server (Active Directory or RADIUS). For more information, see "Authentication Types" on page 261.

5.4 Using Multiple Virtual Networks

When multiple virtual networks are defined, it is important to know how user traffic is matched to a VSC definition.

The following table summarizes how incoming traffic is handled on the service controller. This table assumes that all virtual networks have access control enabled.

Incoming traffic properties	Port	If ...	Then ...
SSID and untagged	LAN	VSC with matching SSID exists	Traffic is sent on the egress mapping defined on the matching VSC
		No VSC with matching SSID exists	Traffic is sent on the egress mapping defined on the default VSC.
SSID and VLAN or VLAN only	LAN or Internet	VSC with matching Ingress VLAN exists.	Traffic is sent on the egress mapping defined on the matching VSC.
		VLAN exists in VLAN table (but is not assigned to a VSC ingress	Traffic is routed according to the global routing table.
		No VLAN exists.	Traffic is blocked.
Untagged	LAN		Traffic is sent on the egress mapping defined on the default VSC.

5.4.0.1 About the Default Virtual Network

The default VSC is the first virtual network that appears in the virtual network list. Initially, this VSC is named **Alvarion Ltd.**

- **When access control is disabled on the default virtual network,** traffic from wired users connected to the service controller’s LAN port is blocked.
- **When access control is enabled on the default virtual network,** traffic from authenticated wired users connected to the service controller’s LAN port is sent on the egress mapping defined on the default virtual network. If HTML and 802.1X based authentication methods are disabled, traffic from all users is sent on the egress mapping without the need for authentication

NOTE

If only MAC-based authentication is defined on the default virtual network, wired users gain access to the network without being authenticated. Wireless users however, must log in because MAC-based authentication applies to wireless users only.

5.5 Quality of Service (QoS)

The service controller features a quality of service (QoS) implementation that provides a wide range of methods for traffic prioritization.

5.5.0.1 QoS Priority Mechanism

The QoS priority mechanism defines four traffic queues based on the WMM standard. In order of priority, these queues are:

Queue	Typically used for
1	Voice traffic
2	Video traffic
3	Best effort data traffic
4	Background data traffic

Each QoS priority option maps traffic to one of the four traffic queues. Users that do not support the QoS priority option defined on a VSC are always assigned to queue 3.

QoS priority is only applied to wireless traffic sent by APs to wireless users with the following exception: If a VSC-based priority setting is selected and egress traffic is assigned to a VLAN then the VSC-based priority settings are mapped to a corresponding 802.1p value for all incoming traffic received from wireless clients and forwarded onto the VLAN. For example, if VSC-based priority **High** is selected, then traffic from wireless clients will be mapped to the appropriate 802.1p value for queue 2.

NOTE

Traffic delivery is based on strict priority (per the WMM standard). Therefore, if excessive traffic is present on queues 1 or 2, it will reduce the flow of traffic on queues 3 and 4.

5.5.0.1.0.1 SVP Support

Spectralink Voice Protocol is an open standard for the prioritization of voice traffic on wireless and wired LANs. SVP traffic is sent on queue 1 for all priority mechanisms except virtual network-based.

5.5.0.2 802.1p

802.1p traffic is classified based on the VLAN priority field present within the VLAN header. When this mechanism is selected, WMM capabilities are advertised, enabling WMM clients to associate and take advantage of them. This setting has no effect on legacy clients.

Queue	Traffic type (based on VLAN priority field)
1	SVP traffic
1	6,7
2	4,5
3	0,2
3	Other traffic
4	1,3

NOTE

To support 802.1p, the VSC must have a VLAN assigned to it.

5.5.0.3 VSC-based Priority

The VSC-based priority mechanism is unique to Alvarion Ltd. APs. It enables you to specify a priority level for all traffic on a virtual network. This enables users that do not have a QoS mechanism to set traffic priority by connecting to the appropriate SSID.

If you enable a virtual network-based priority mechanism, it takes precedence regardless of the priority mechanism supported by associated users. For example, if you set **VSC-Based Low Priority** for a VSC, all devices that connect to the virtual network have their traffic set at this priority.

Queue	Description
1	Very High
2	High
3	Normal
4	Low

NOTE

Alvarion Ltd. strongly recommends that you reserve **VSC-Based Very-high** priority for voice applications.

5.5.0.4 Differential Services (DiffServ)

Differential services is a method for defining IP traffic priority on a per-hop basis. The Differential Service bits are defined in RFC2474 and are composed of the six most significant bits of the IP TOS field. These bits define the class selector code points which maps to the appropriate traffic queue.

Queue	Traffic type (based on binary value of Class Selector Codepoint)
1	SVP traffic
1	111000 (Network control)
1	110000 (Internetwork control)
2	101000 (Critical)
2	100000 (Flash override)
3	011000 (Flash)
3	000100 (Routine)
4	010000 (Immediate)
4	001000 (Priority)
3	Other traffic

5.5.0.5 TOS

The IP TOS (type of service) field can be used to mark prioritization or special handling for IP packets.

Queue	Traffic type
1	SVP traffic
1	0x30, 0xE0, 0x88, 0xB8
2	0x28, 0xA0
3	0x08, 0x20
3	Non-TOS traffic
4	All other TOS traffic

5.5.0.6 IP QoS

This option lets you assign traffic to the queues based on the criteria in one or more IP QoS profiles. For more information, see “IP QoS” on page 187.

5.5.0.7 Disabled

When QoS traffic prioritization is disabled, all traffic on the virtual network is sent to queue 3.

5.5.0.8 QoS example

In this QoS example a single service controller provides voice and data wireless support with different quality of service settings for guests and employees.

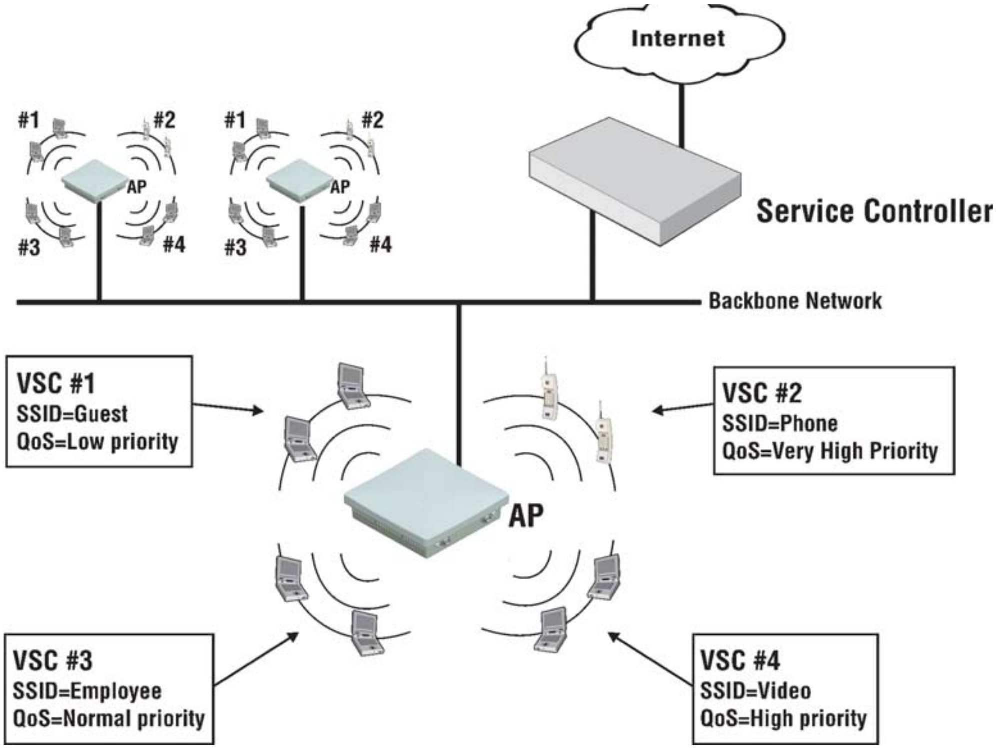


Figure 5-29: QoS Example

VSCs define the following SSIDs:

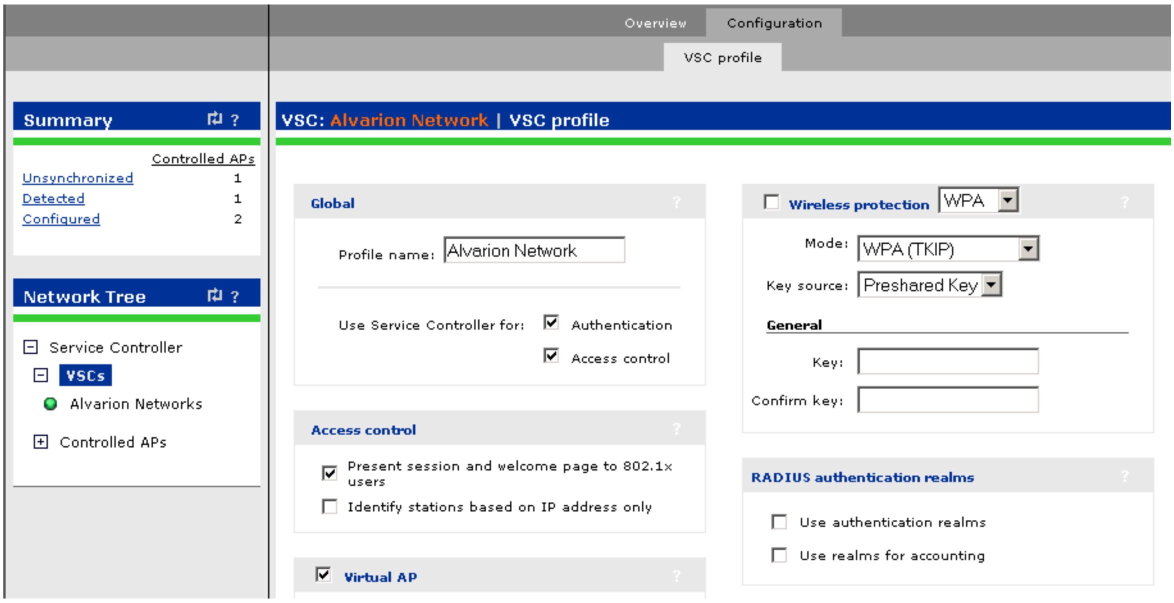
- **Phone**: Supports wireless phones using very high priority.
- **Video**: Supports high-priority video traffic for video conferences.
- **Employee**: Used by employees. Features a higher QoS setting than the guest profile.
- **Guest**: Used by guests. Guest get the lowest traffic priority, to reserve bandwidth for employees.

IMPORTANT

For more examples of QoS implementation, see the Deployment Guide.

5.6 Creating a New Virtual Network

To add a VSC, select **Service Controller** > **virtual networks** > **Add New VSC Profile**.



	Controlled APs
Unsynchronized	1
Detected	1
Configured	2

Global

Profile name: Alvarion Network

Use Service Controller for: ☑ Authentication ☑ Access control

Access control

☑ Present session and welcome page to 802.1x users

□ Identify stations based on IP address only

☑ Virtual AP

□ Wireless protection WPA

Mode: WPA (TKIP)

Key source: Preshared Key

General

Key:

Confirm key:

RADIUS authentication realms

□ Use authentication realms

□ Use realms for accounting

Figure 5-30: Creating a New Virtual Network

Define VSC parameters and select **Save**. Familiarize yourself with sections of interest in “Virtual Network Configuration Options” on page 105. Refer to the online help for parameter descriptions.

5.7 Assigning a Virtual Network to a Group

When working with controlled APs, virtual network definitions must be bound to a group so that they will automatically be activated on the APs in the group. For information on how to bind (assign) a VSC to group, see "Binding a Virtual Network to a Group" on page 67

NOTE

When working with autonomous APs, the virtual network definition you create on the service controller must be manually configured on each autonomous AP. See "Working with Autonomous APs" on page 325 and the *AP Admin Guide* for details.

TIP

The Deployment Guide provides numerous detailed examples on virtual network configuration when using the service controller with both controlled and autonomous APs.

6

Chapter 6 - Wireless Mobility

In This Chapter:

6.1 Key Concepts

Alvarion service controllers include basic Layer 2 (L2) mobility support allowing wireless users to roam between Alvarion APs within the same subnet. The optional Mobility license enhances basic wireless mobility by adding two separate features, WPA2 Opportunistic Key Caching and L3 Mobility.

6.1.1 WPA2 Opportunistic Key Caching

Using optimizations of 802.1X/802.11i authentication, WPA2 Opportunistic Key Caching enables a wireless client to perform a full RADIUS authentication once and then re-use those authentication credentials on each subsequent roam without the need to re-authenticate through RADIUS. The service controller maintains updated key information on APs based on the Mobility Neighborhood so that a wireless user can roam between APs without incurring a full 802.1X RADIUS handshake delay.

WPA2 Opportunistic Key Caching provides secure and fast user authentication based on the WPA2 and 802.1X standards. It:

- Eliminates delays associated with reauthentication.
- Provides hand-offs in less than 50 milliseconds, as required for time-sensitive services such as voice.
- Preserves a user's RADIUS-assigned parameters such as security, QoS ,and VLAN, enabling smooth transition of all services to which the user has access.

6.1.1.1 How It Works

With WPA 2 Opportunistic key caching, each wireless client has one set of encryption keys that are shared by all APs in the “mobility neighborhood.” When a client roams to a new AP, it sends a PMKID (see IEEE 802.11i for more information) with its reassociation request. If this PMKID matches the encryption keys for that client, then the client is able to bypass RADIUS authentication and move directly to the 4-way encryption handshake.

NOTE

The wireless client software must support Opportunistic Key Caching. The Microsoft windows wireless client and the Juniper Odyssey client both support this.

6.1.2 Layer 3 Mobility

Layer 3 (L3) mobility enables users to roam between APs that are connected to different service controllers operating on different subnets, while maintaining their assigned IP address. L3 mobility enables a seamless wireless infrastructure to be deployed across a routed backbone network while delivering a consistent set of services to users, regardless of the subnets used for the underlying infrastructure. L3 mobility uses a unique technology set that eliminates the need for special client software required by some competing solutions.

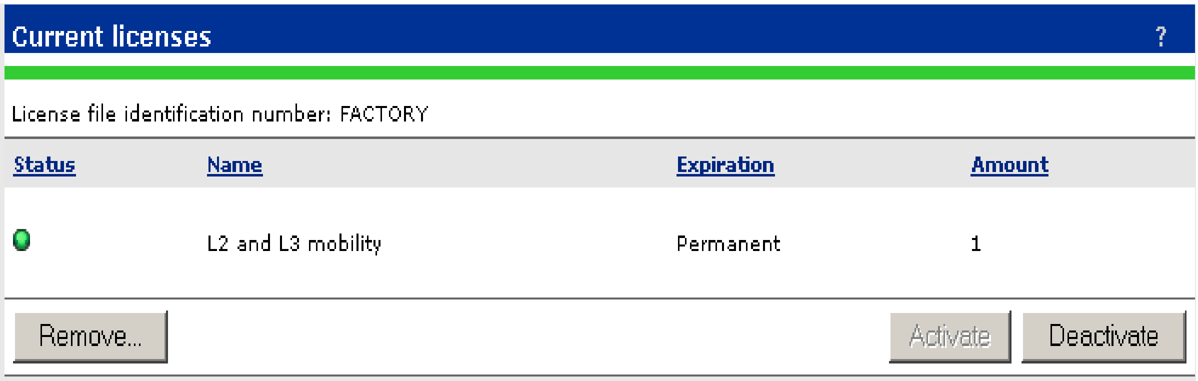
6.1.2.1 How It Works

The mobility feature defines a mobility domain, which is an interconnection between up to four service controllers for the purpose of exchanging mobility information on roaming users. One service controller must be defined as the primary mobility controller. It acts as the central site for distribution of mobility information. The primary controller must be reachable via the LAN port on all other service controllers that are part of the mobile domain. (Internet port connections are not supported.)

6.1.3 The Mobility License

If you purchased the AOS Mobility Pack at the same time that you purchased your service controller, the license is factory-installed. You do not need to install a license. When you purchase a AOS Mobility Pack separately, you are provided with a license file.

To verify that the AOS Mobility Pack is installed, select **Service Controller** >> **Maintenance** > **Licenses** and confirm that there is an “L2 and L3 mobility” license installed.



Current licenses

License file identification number: FACTORY

Status	Name	Expiration	Amount
●	L2 and L3 mobility	Permanent	1

Figure 6-1: Mobility License

For information on how to work with and install licenses, see “Licenses” on page 345.

6.2 Wireless Mobility Scenario

This section walks you through the minimum configuration steps necessary to implement a simple mobility scenario with support for Opportunistic key caching and L3 Mobility. Once implemented, wireless clients, including Wi-Fi phones, can roam between APs on different subnets without experiencing delays as the wireless client is switched from one AP to the other. The scenario is illustrated as follows:

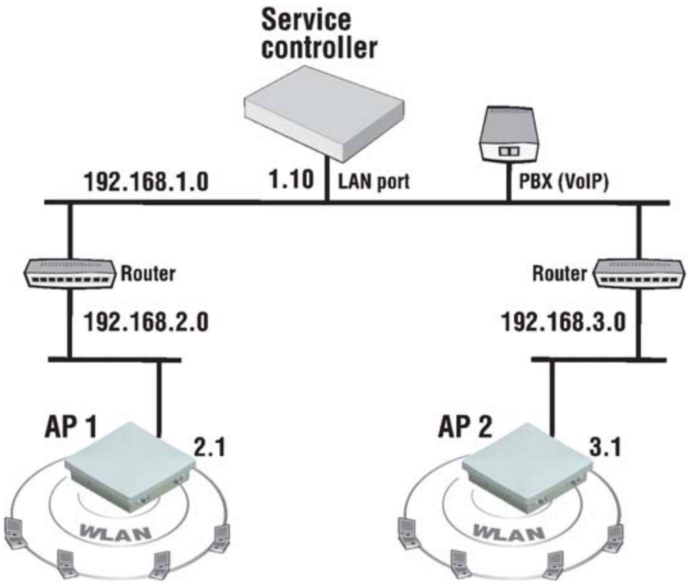


Figure 6-2: Wireless Mobility Scenario

The following items are required to implement this scenario:

- One Wi² series service controller such as the Wi²-CTRL-10 with optional Mobility license installed.
- Two APs such as the Wi² AP.
- A PBX / VoIP server.
- A voice-capable wireless client such as a Wi-Fi phone.
- Multiple subnets connected by router. This scenario uses three subnets: 192.168.1.0, 192.168.2.0, and 192.168.3.0.

- A DHCP scope defined for each subnet.

To configure the network

1 Using appropriate router and DHCP server configuration (beyond the scope of this document) construct a three-subnet network as illustrated above with the service controller (LAN port) on subnet **192.168.1.0**, one Wi² AP on subnet **192.168.2.0** and another on subnet **192.168.3.0**.

To pre-configure the service controller

The service controller LAN port defaults to IP address 192.168.1.1. You will likely need to change this address to an available address on subnet 192.168.1.0. Before connecting the service controller to your network, pre-configure its IP address as follows:

1 Take note of the service controller MAC address (label on the service controller cabinet and in its management tool on page **Service Controller** > **Network** > **Ports**).

2 Using the MAC address noted in step 1, Reserve an IP address for the service controller in the DHCP server responsible for subnet 192.168.1.0.

1 Reset the service controller to its factory defaults. In its management tool, select **Service Controller** >> **Maintenance** > **Config file management**. For additional information see Resetting to Factory Defaults.

2 Set your computer IP address to a value in the range 192.168.1.2 to 192.168.1.254.

3 Disconnect any cable from the service controller Internet port and connect the service controller LAN port to your computer.

4 In a web browser, open page: **https://192.168.1.1**.

5 Select **Service Controller** > **Network** > **Ports** > **LAN port** and under **Addressing**, set an available **Static IP address** (**192.168.1.10** in this scenario) and **Mask**. After selecting **Save**, you will lose connection with the management tool. This is expected behavior.

To connect the service controller to the network

1 Connect the service controller LAN port to the network on which it will reside (subnet 192.168.1.0).

2 Configure your computer's wired LAN port for Automatic IP address assignment by DHCP and connect it to the same 192.168.1.0 subnet.

3 In a web browser open page **https://**<IP address of your service controller>. Confirm that the management tool opens. This is sufficient to prove that the service controller is reachable on the network via its LAN port.

4 Connect the service controller Internet port to an Internet firewall or broadband router. By default, the Internet port has its DHCP client enabled. If necessary, change the Internet port's addressing (**Service Controller** >> **Network** > **Ports** > **Internet port**).

5 Confirm that the Internet is reachable. On page **Service Controller** >> **Tools** > **Ping**, ping a public web site that responds to pings such as **yahoo.com**.

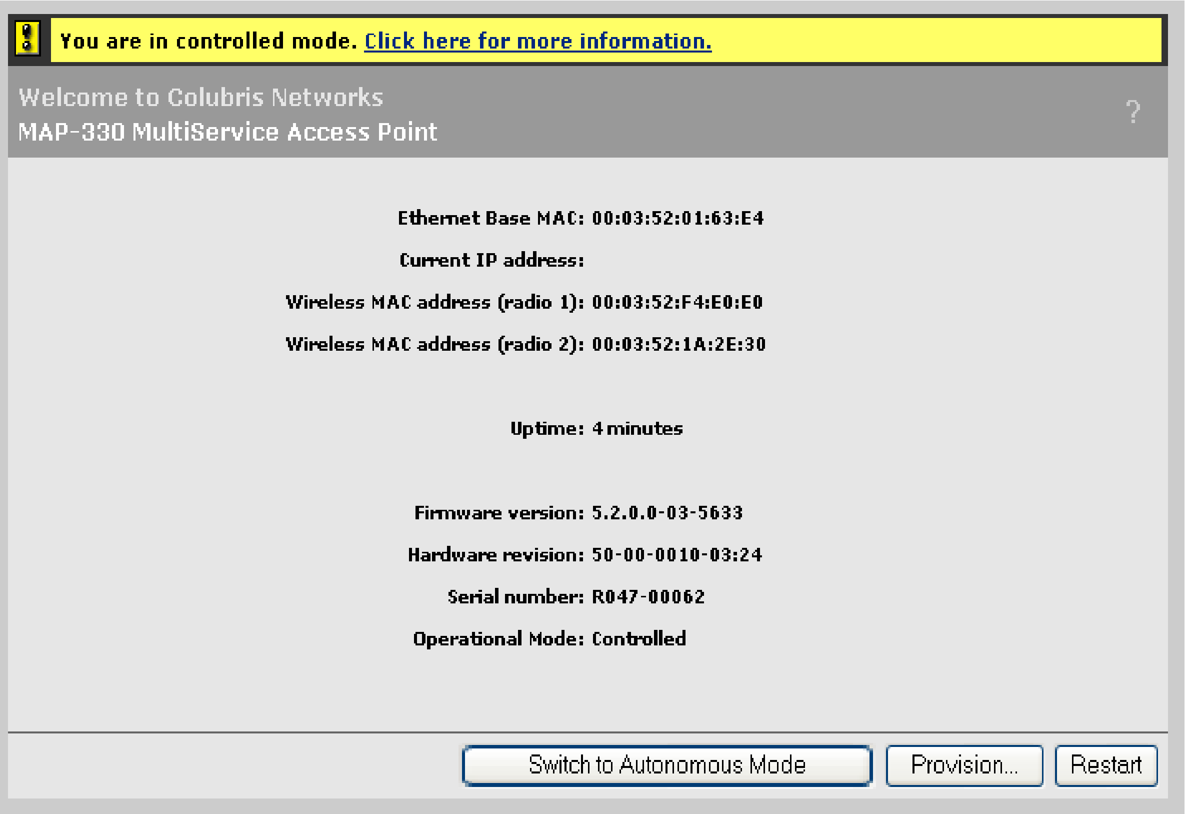
➤ **To provision the APs**

The two APs need to be provisioned so that they can find the service controller that will manage them across the routers. Before connecting the APs to the network, provision them as follows:

1 Reset the AP to its factory default state. Power-on the AP without any Ethernet cables connected, and press and hold the Reset switch until the status lights flash on and off three times. For details, see "*Resetting to factory defaults*" in the *Wi² AP Admin Guide.*

2 Using a crossover cable, connect your computer to Port 1 of the AP.

3 In a web browser, open the AP's management tool at **https://192.168.1.1**. The controlled mode home page opens, like this:



You are in controlled mode. Click here for more information.

Welcome to Colubris Networks
MAP-330 MultiService Access Point

Ethernet Base MAC: 00:03:52:01:63:E4

Current IP address:

Wireless MAC address (radio 1): 00:03:52:F4:E0:E0

Wireless MAC address (radio 2): 00:03:52:1A:2E:30

Uptime: 4 minutes

Firmware version: 5.2.0.0-03-5633

Hardware revision: 50-00-0010-03:24

Serial number: R047-00062

Operational Mode: Controlled

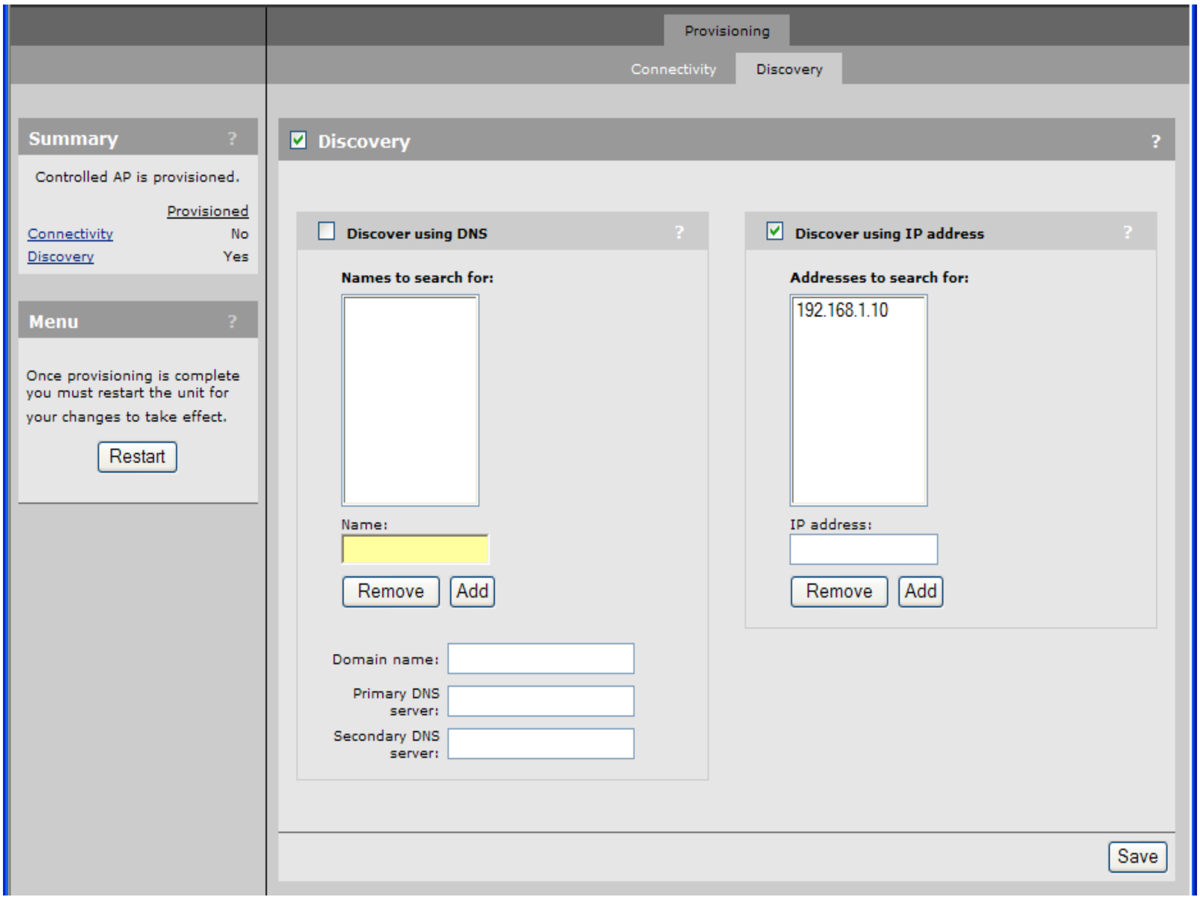
Figure 6-3: Controlled Mode Homepage

4 Select **Provision** at the bottom of the home page and then select the **Discovery** tab.

NOTE

The **Provision** button is only available if the AP is in its factory-default state.

5 Set the **Discovery** and **Discover using IP address** check boxes.



Controlled AP is provisioned.

	Provisioned
Connectivity	No
Discovery	Yes

Once provisioning is complete you must restart the unit for your changes to take effect.

☑ Discovery

□ Discover using DNS

Names to search for:

Domain name:

Primary DNS server:

Secondary DNS server:

☑ Discover using IP address

Addresses to search for: 192.168.1.10

Figure 6-4: Provisioning Page

6 Under IP address specify the IP address of the service controller configured in step A.7 above and select **Add.** Select **Save**.

7 Disconnect the power and Ethernet cables from the first AP and repeat steps 1 to 6 for the second AP.

Both APs are now provisioned to find the service controller across the routers.

To connect each AP to its subnet

As described here, connect one AP to subnet 192.168.2.0 and the other to subnet 192.168.3.0.

1 Connect Port 1 of AP 1 to subnet 192.168.2.0.

2 Connect Port 1 of AP 2 to subnet 192.168.3.0.

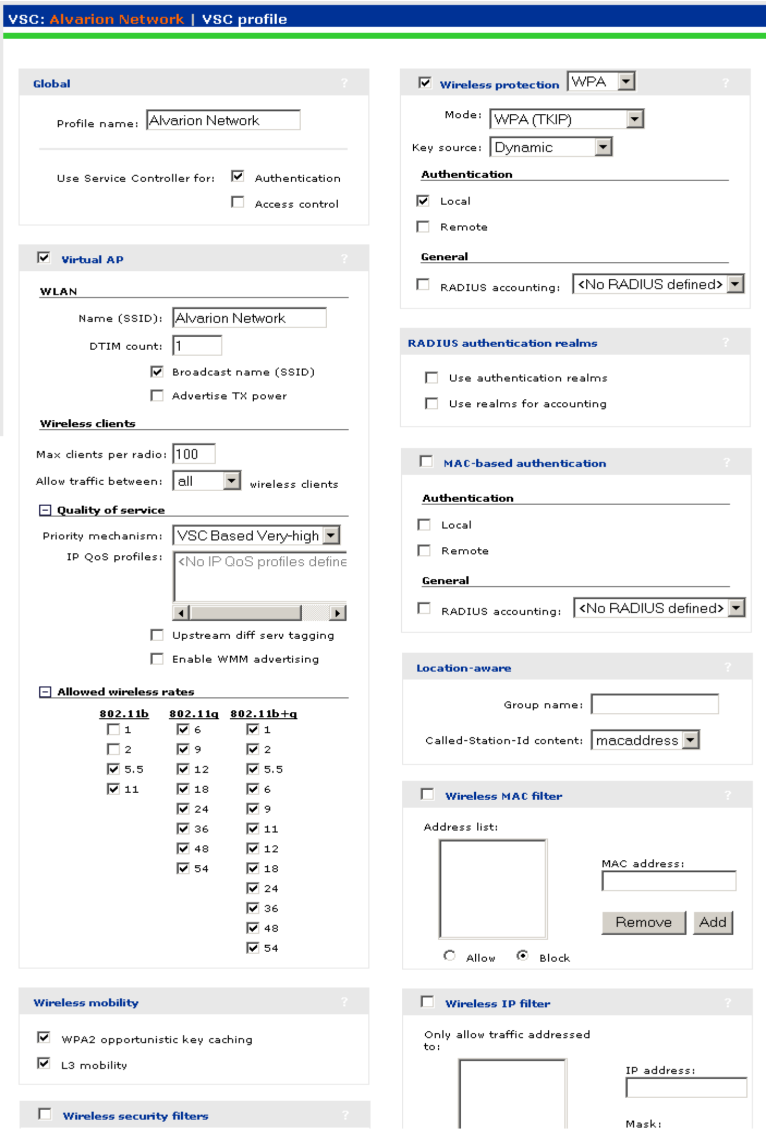
In the service controller management tool, verify that both APs get discovered by the service controller

NOTE

For testing purposes ensure that the two APs are as far apart as possible but no more than 100 feet (31 meters).

To configure a virtual network profile

1 In the service controller management tool, open the virtual network profile that you will use for mobility, and configure the following highlighted items:



VSC: Alvarion Network | VSC profile

Global

Profile name: Alvarion Network

Use Service Controller for: ☑ Authentication ☐ Access control

☑ Virtual AP

WLAN

Name (SSID): Alvarion Network

DTIM count: 1

☑ Broadcast name (SSID)

☐ Advertise TX power

Wireless clients

Max clients per radio: 100

Allow traffic between: all wireless clients

Quality of service

Priority mechanism: VSC Based Very-high

IP QoS profiles: <No IP QoS profiles define

☐ Upstream diff serv tagging

☐ Enable WMM advertising

Allowed wireless rates

802.11b	802.11g	802.11b+g
☐ 1	☑ 6	☑ 1
☐ 2	☑ 9	☑ 2
☑ 5.5	☑ 12	☑ 5.5
☑ 11	☑ 18	☑ 6
	☑ 24	☑ 9
	☑ 36	☑ 11
	☑ 48	☑ 12
	☑ 54	☑ 18
		☑ 24
		☑ 36
		☑ 48
		☑ 54

Wireless mobility

☑ WPA2 opportunistic key caching

☑ L3 mobility

☐ Wireless security filters

☑ Wireless protection WPA

Mode: WPA (TKIP)

Key source: Dynamic

Authentication

☑ Local

☐ Remote

General

☐ RADIUS accounting: <No RADIUS defined>

RADIUS authentication realms

☐ Use authentication realms

☐ Use realms for accounting

☐ MAC-based authentication

Authentication

☐ Local

☐ Remote

General

☐ RADIUS accounting: <No RADIUS defined>

Location-aware

Group name:

Called-Station-Id content: macaddress

☐ Wireless MAC filter

Address list:

MAC address:

○ Allow ● Block

☐ Wireless IP filter

Only allow traffic addressed to:

IP address:

Mask:

Figure 6-5: Configuring a Virtual Network Profile

NOTE

For details on each option, consult the online help.

NOTE

This example uses the service controller’s internal RADIUS server which is enabled by default.

2 Under **Global**, clear **Access control**.

3 Select **Wireless protection** and configure its options as follows:

   a Set Wireless protection to **WPA.**

   b Set **Mode** to **WPA2 (AES/CCMP)**.

   c Set **Key source** to **Dynamic**

   d Set **Authentication** to **Local**.

5 Under **Virtual AP: Quality of service**, configure the following:

   a Set **Priority mechanism** to **VSC Based Very high**. This is important for voice services.

   b Unless your network requires it, clear **Upstream diff serv tagging**.

   c Unless your Wi-Fi phones specifically support Wi-Fi Multimedia, clear **Enable WMM advertising**.

4 Under **Virtual AP: Allowed wireless rates**, clear all speeds below 5.5Mbps. Affects 802.11b and 802.11g.

5 Under **Wireless mobility**, select **WPA2 opportunistic key caching** and **L3 mobility**.

NOTE

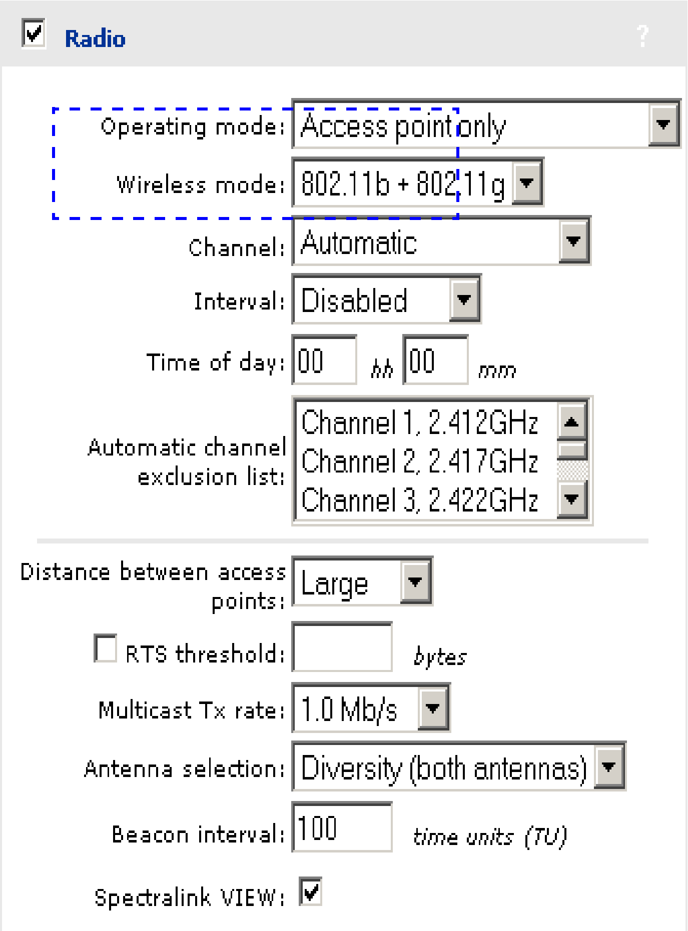
If the Wi-Fi phones that you will use support only pre-shared key static encryption (Spectralink for example), do not enable **WPA2 opportunistic key caching**.

Clear **Wireless security filters..**

To configure the radios

Configure the radios of both APs as indicated here.

1 Select **Service Controller** > **Controlled APs** >> **Configuration** > **Single radio** and configure the following highlighted items.



☑ Radio

Operating mode: Access point only

Wireless mode: 802.11b + 802.11g

Channel: Automatic

Interval: Disabled

Time of day: 00 *hh* 00 *mm*

Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz

Distance between access points: Large

□ RTS threshold: *bytes*

Multicast Tx rate: 1.0 Mb/s

Antenna selection: Diversity (both antennas)

Beacon interval: 100 *time units (TU)*

Spectralink VIEW: ☑

Figure 6-6: Configuring a Single Radio

2 Set **Operating mode** to **Access point only**.

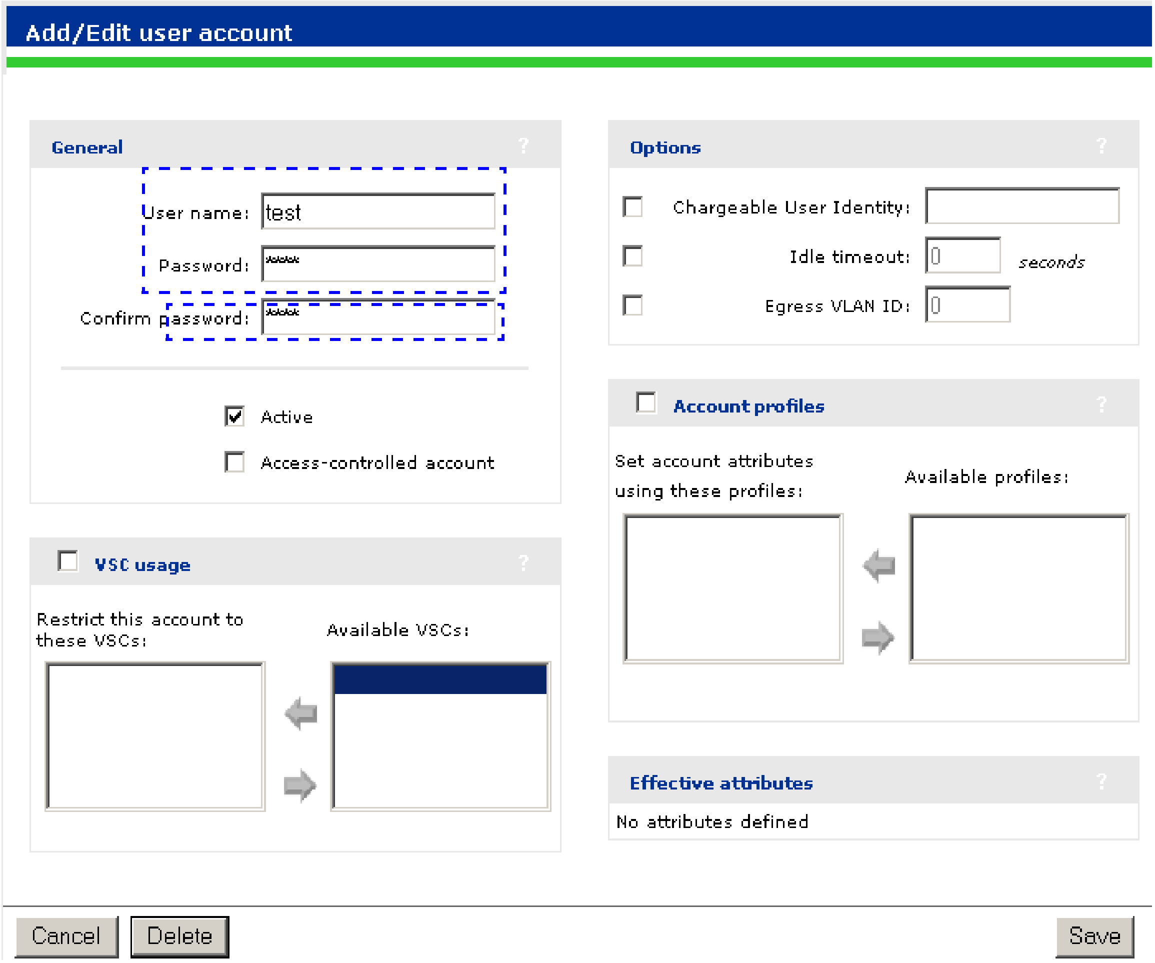
3 Set **Wireless mode** according to phone type. It is recommended that you select **802.11b + 802.11g** even if your phones only support 802.11b.

4 Set **Distance between access points** to **Large**.

5 Regardless of phone type, select **Spectralink View** for all voice applications. This causes undeliverable frames to be discarded sooner than normal which is desirable for voice.

To add a user

1 On page **Service Controller >> Users > User Accounts**, add a test user as highlighted:



Add/Edit user account

General

User name: test

Password: ****

Confirm password: ****

☑ Active

□ Access-controlled account

□ VSC usage

Restrict this account to these VSCs:

Available VSCs:

Options

□ Chargeable User Identity:

□ Idle timeout: 0 seconds

□ Egress VLAN ID: 0

□ Account profiles

Set account attributes using these profiles:

Available profiles:

Effective attributes

No attributes defined

Figure 6-7: Adding a User

2 Under **General**, fill in **User name**, and **Password**.

3 Clear **Access-controlled account**.

To test with a Wi-Fi phone

You can follow these basic steps to test your Mobility network with a Wi-Fi phone.

If you enabled **WPA2 Opportunistic Key Caching** in step **F.6** above, test with a Wi-Fi phone that supports this such as the **Hitachi WIP-5000-EA**.

Otherwise, test with a Wi-Fi phone that supports pre-shared key (static encryption).

1 Configure your Wi-Fi phone to use wireless network “Corporate” and user “test”. If applicable, configure the phone to use **WPA2 Opportunistic Key Caching**.

2 Although the network is set up to assign an IP address to the phone via DHCP you may wish to initially assign a static IP address to the phone. Be sure to us an available address outside of the range of addresses being assigned by the DHCP server.

3 Position yourself as far away as possible from the second AP (AP 2) but within good range of the first AP (AP 1).

4 Initiate a voice call and commence a conversation with someone.

5 Move away from AP 1 and close to AP 2 to force roaming, while continuing to talk (or listen).

NOTE

If the APs are close together (a few feet / meters apart) you can still force roaming by manipulating the antennas. Initially connect one antenna to AP 1 and no antenna to AP 2. Begin a voice call via AP 1 and then attach one antenna to AP 2. Then, remove the antenna from AP 1 to force the roam to AP 2.

6 Confirm that the phone call is not interrupted during the hand off from AP 1 to AP 2.

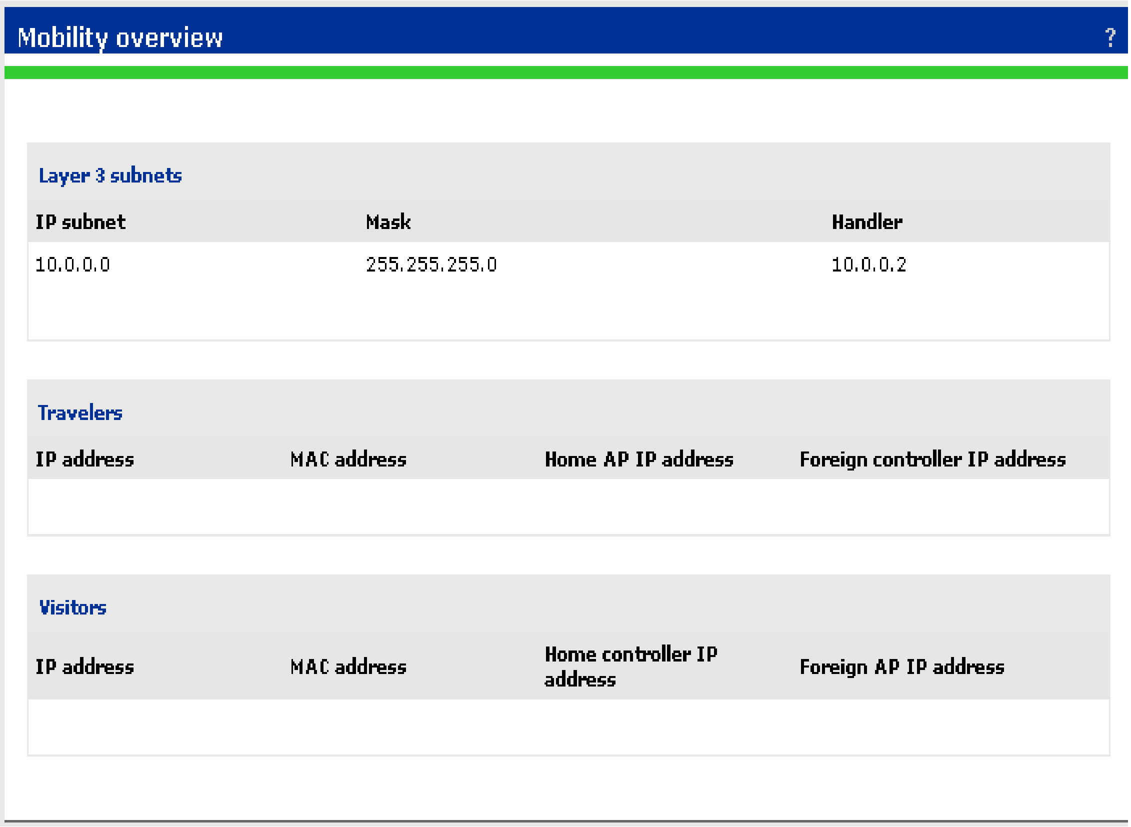
7 If you wish, return to the original AP while continuing to talk, again confirming smooth hand off back to AP 1.

In the service controller management tool you can see with which AP a particular wireless client is associated. Open page **Service Controller** > **Controlled APs** >> **Overview** > **Wireless client** and look for the MAC address of the Wi-Fi phone you are testing.

You can view L3 mobility information on page **Service Controller** >> **Status** > **L3 mobility**.

The following sample L3 mobility status page shows how it looks after the Wi-Fi phone (IP address 192.168.2.100) has roamed from its home AP (AP 1 at 192.168.2.1) to the foreign AP (AP 2 at 192.168.3.1). The phones IP address of 192.168.2.100 is retained when it roams to AP 2.

The service controller uses IP address 192.168.1.10, and since there is only one service controller, both the Home and Foreign addresses are the same.



Mobility overview ?

Layer 3 subnets

IP subnet	Mask	Handler
10.0.0.0	255.255.255.0	10.0.0.2

Travelers

IP address	MAC address	Home AP IP address	Foreign controller IP address

Visitors

IP address	MAC address	Home controller IP address	Foreign AP IP address

Figure 6-8: L3 Mobility Status Page

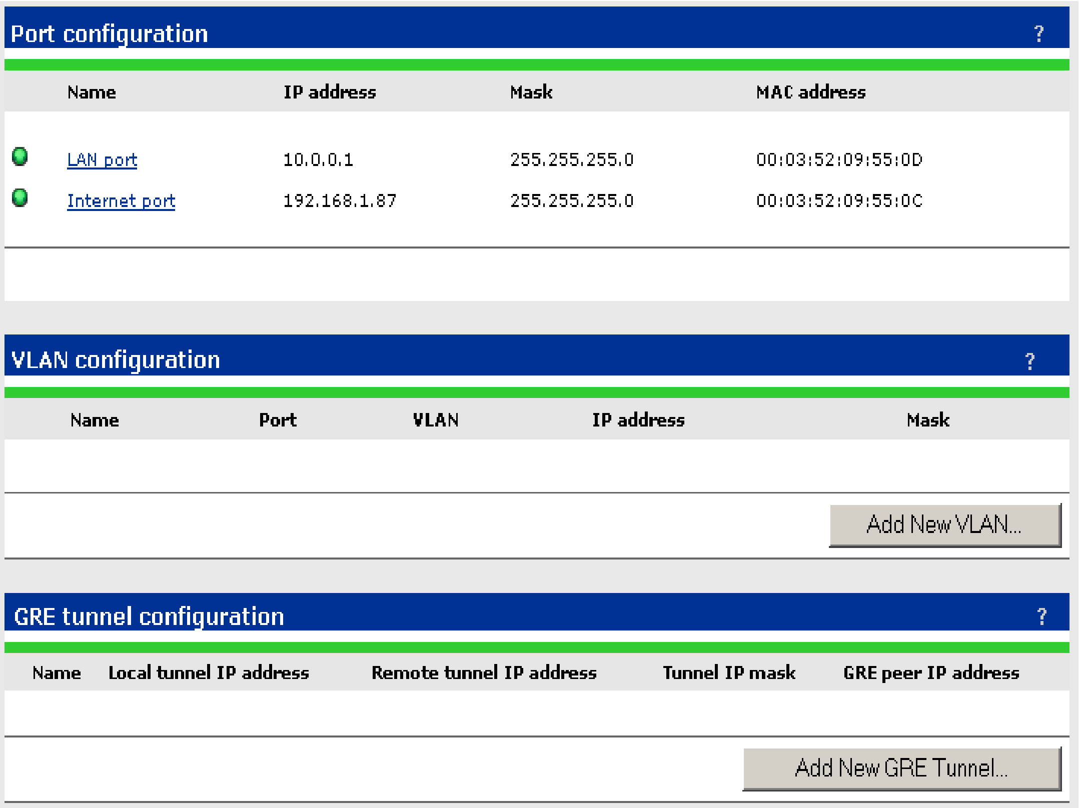
7

Chapter 7 - Network Configuration

In This Chapter:

7.1 Port Configuration

The **Port configuration** page displays summary information about all ports, VLANs, and GRE tunnels. Open this page by selecting **Service Controller >> Network > Ports**.



Port configuration ?

	Name	IP address	Mask	MAC address
●	LAN port	10.0.0.1	255.255.255.0	00:03:52:09:55:0D
●	Internet port	192.168.1.87	255.255.255.0	00:03:52:09:55:0C

VLAN configuration ?

Name	Port	VLAN	IP address	Mask

GRE tunnel configuration ?

Name	Local tunnel IP address	Remote tunnel IP address	Tunnel IP mask	GRE peer IP address

Figure 7-1: Port Configuration

7.1.1 Port Configuration Information

- **Status indicator:** Operational state of each port, as follows:
  - » **Green:** Port is properly configured and ready to send and receive data.
  - » **Red:** Port is not properly configured or is disabled.
- **Name**: Identifier for the port. To configure a port, click its name.
- **IP address**: IP addresses assigned to the port. An address of **0.0.0.0** means that no address is assigned.

- **Mask**: Subnet mask for the IP address.
- **MAC address**: MAC address of the port.

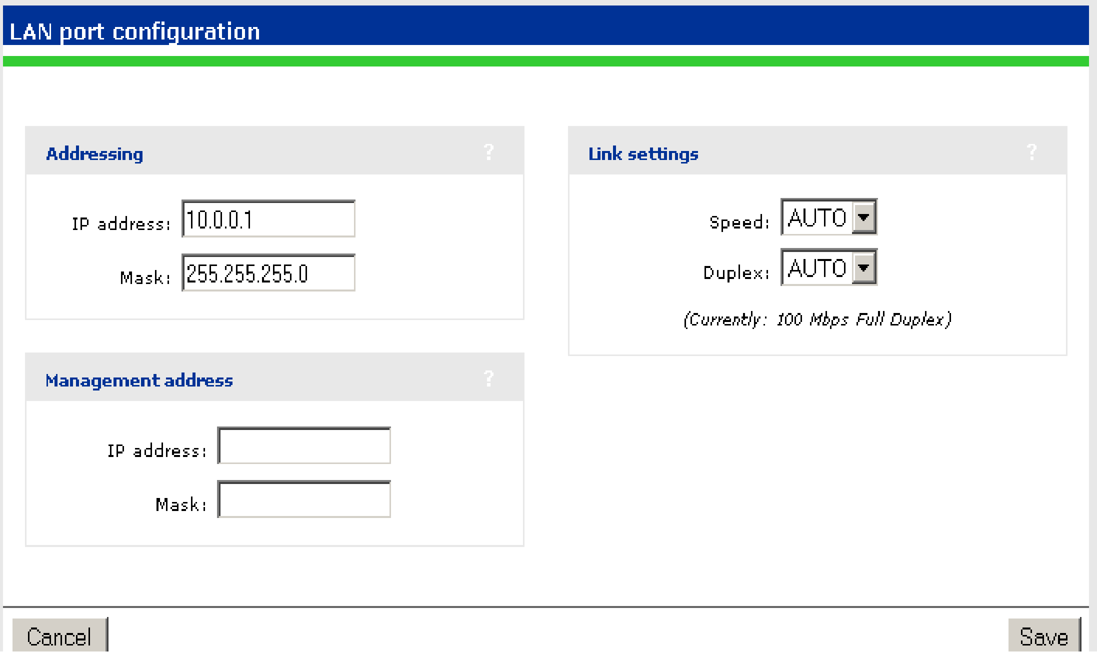
7.1.2 Default Port Settings

By default, ports are configured as follows:

Port	Default IP address	Default DHCP server status
LAN	192.168.1.1	Disabled.
Internet	DHCP client	This feature is not available on the Internet port.

7.1.3 LAN Port Configuration

The LAN port is used to connect the service controller to a wired network. To verify and possibly adjust LAN port configuration, select **Service Controller >> Network** > **Ports** > **LAN port**.



IP address: 10.0.0.1

Mask: 255.255.255.0

Speed: AUTO

Duplex: AUTO

(Currently: 100 Mbps Full Duplex)

IP address:

Mask:

Figure 7-2: LAN Port Configuration

7.1.3.1 Addressing Options

The LAN port must be configured with a static IP address, because the service controller cannot function as a DHCP client on the LAN port. By default it is set to the address 192.168.1.1

For information on configuring address allocation on the LAN port via DHCP server or DHCP relay agent, see "Address Allocation" on page 157.

7.1.3.2 Management Address

Use this option to assign a second IP address to the LAN port. When working with autonomous APs, this address provides a simple way to separate management traffic from user traffic without using VLANs.

For example, by default the LAN port is set to 192.168.1.1 and all client devices obtain an address on this subnet from the service controller`s DHCP server. With this feature you can add another address, say 192.168.2.1/255.255.255.0. Autonomous APs can then be assigned to this subnet using static IP addressing. Now all management traffic exchanged between the service controller and the APs is on a separate subnet.

NOTE

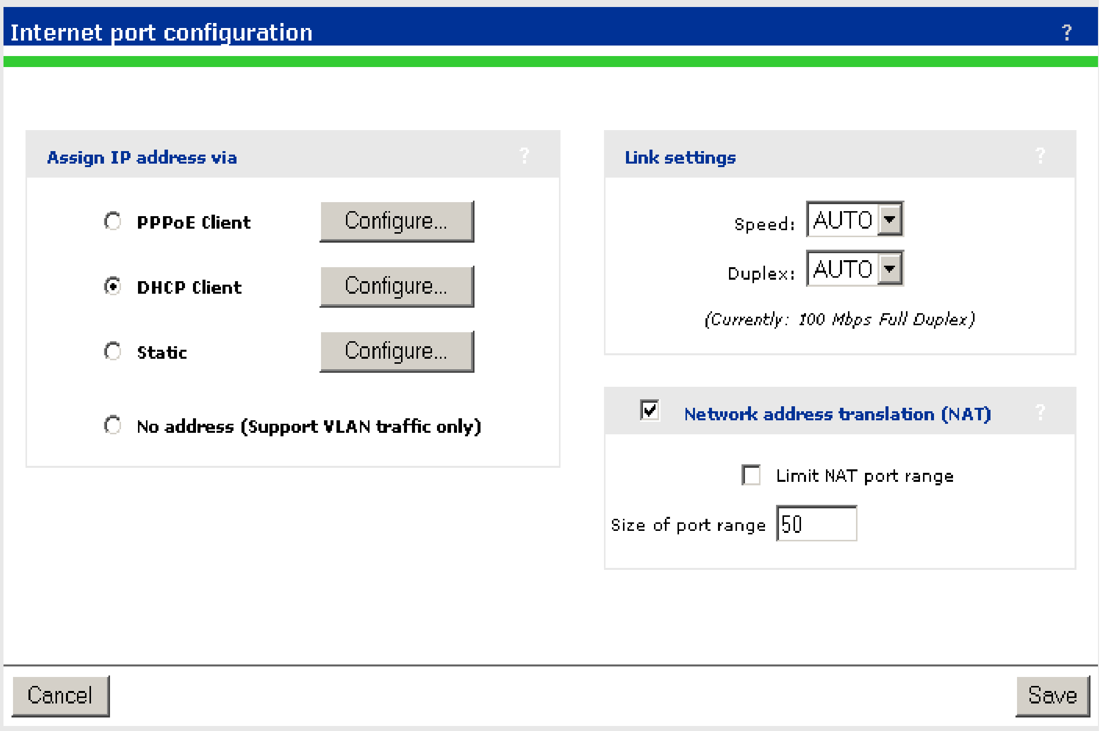
To use this address to access the management tool via the LAN port you will be required to login via the public access interface first.

7.1.3.3 Link Settings

By default, the service controller automatically adjusts link settings based on the type of equipment the port is connected to. If needed, you can force the port to operate at a particular speed or duplex setting.

7.1.4 Internet Port Configuration

To verify and possibly adjust Internet port configuration, select **Service Controller** >> **Network** > **Ports** > **Internet port**.



Internet port configuration ?

Assign IP address via ?

○ PPPoE Client [Configure...]

● DHCP Client [Configure...]

○ Static [Configure...]

○ No address (Support VLAN traffic only)

Link settings ?

Speed: AUTO

Duplex: AUTO

(Currently: 100 Mbps Full Duplex)

☑ Network address translation (NAT) ?

□ Limit NAT port range

Size of port range 50

[Cancel] [Save]

Figure 7-3: Internet Port Configuration

7.1.4.1 Addressing Options

The Internet port supports the following addressing options:

- PPPoE client
- DHCP client (default setting)
- Static addressing
- No address

By default, the Internet port operates as a DHCP client. Select the addressing option that is required by your ISP or network administrator and then select **Configure**. Refer to the online help for descriptions of all configuration options.

7.1.4.2 Link Settings

By default, the service controller automatically adjusts link settings based on the type of equipment the port is connected to. If needed, you can force the port to operate at a particular speed or duplex setting.

7.1.4.3 Network Address Translation

Enable this option to permit all the computers on the network to simultaneously share the connection on the Internet port. For more information, see "Network Address Translation (NAT)" on page 181.

7.1.4.3.1 Limit NAT Port Range

When enabled, the service controller reserves a range of TCP and UDP ports for each authenticated user starting at port 5000, and maps all outgoing traffic for the user within the range.

NOTE

Enabling this feature only affects outgoing TCP/UDP traffic. Applications that set an incoming port (Active FTP, for example) may select a port that is outside of the allocated port range.

NOTE

If you enable this feature you should not assign static NAT mappings in the range 5000 to 10000.

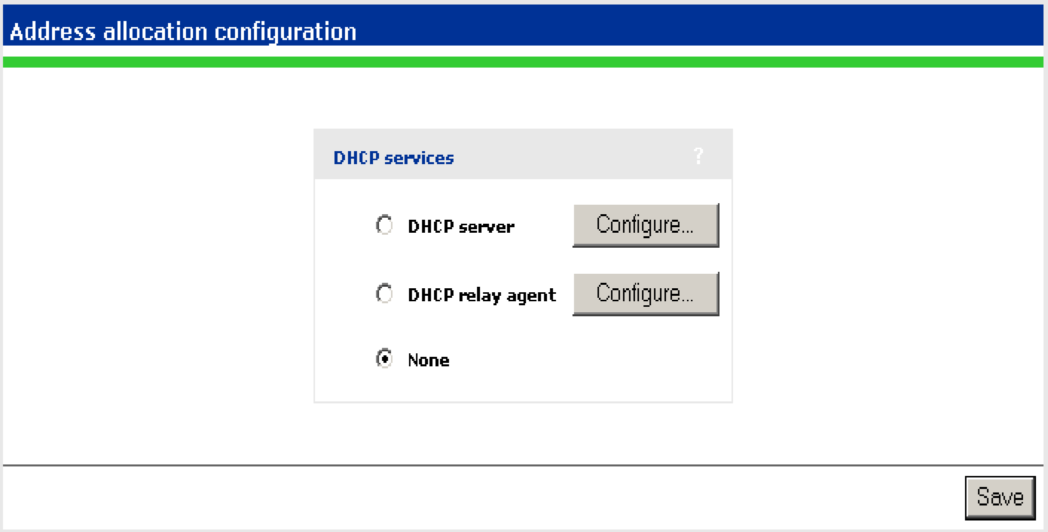
7.1.4.3.2 Size of Port Range

Sets the number of TCP and UDP ports reserved for each user.

7.2 Address Allocation

The service controller can operate as a DHCP server or DHCP relay agent on the LAN port. This enables it to assign IP addresses to downstream devices connected to the LAN port.

By default, address allocation is disabled. To configure address allocation settings, select **Service Controller** >> **Network** > **Address allocation**.



Address allocation configuration

DHCP services

○ DHCP server

○ DHCP relay agent

● None

Figure 7-4: Address Allocation

7.2.1 DHCP Server (Global)

The global DHCP server can be used to automatically assigning IP addresses to devices that are connected to the service controller via the LAN port.

NOTE

Do not enable the DHCP server if the LAN port is connected to a network that already has an operational DHCP server.

A separate DHCP server can also be enabled on each virtual network to assign addresses to users. For details, see “DHCP Server” on page 117.

The host name in the currently installed SSL certificate is automatically assigned as the domain name of the service controller. The factory default SSL certificate that is installed on the service controller has the host name **wireless.alvarion.com**.

You do not have to add this name to your DNS server for it to be resolved. The service controller intercepts all DNS requests it receives. It resolves any request that matches the certificate host name by returning the IP address assigned to the Internet port. All other DNS requests are forwarded to the appropriate DNS servers as configured on the **Service Controller** > **Network** > **DNS** page.

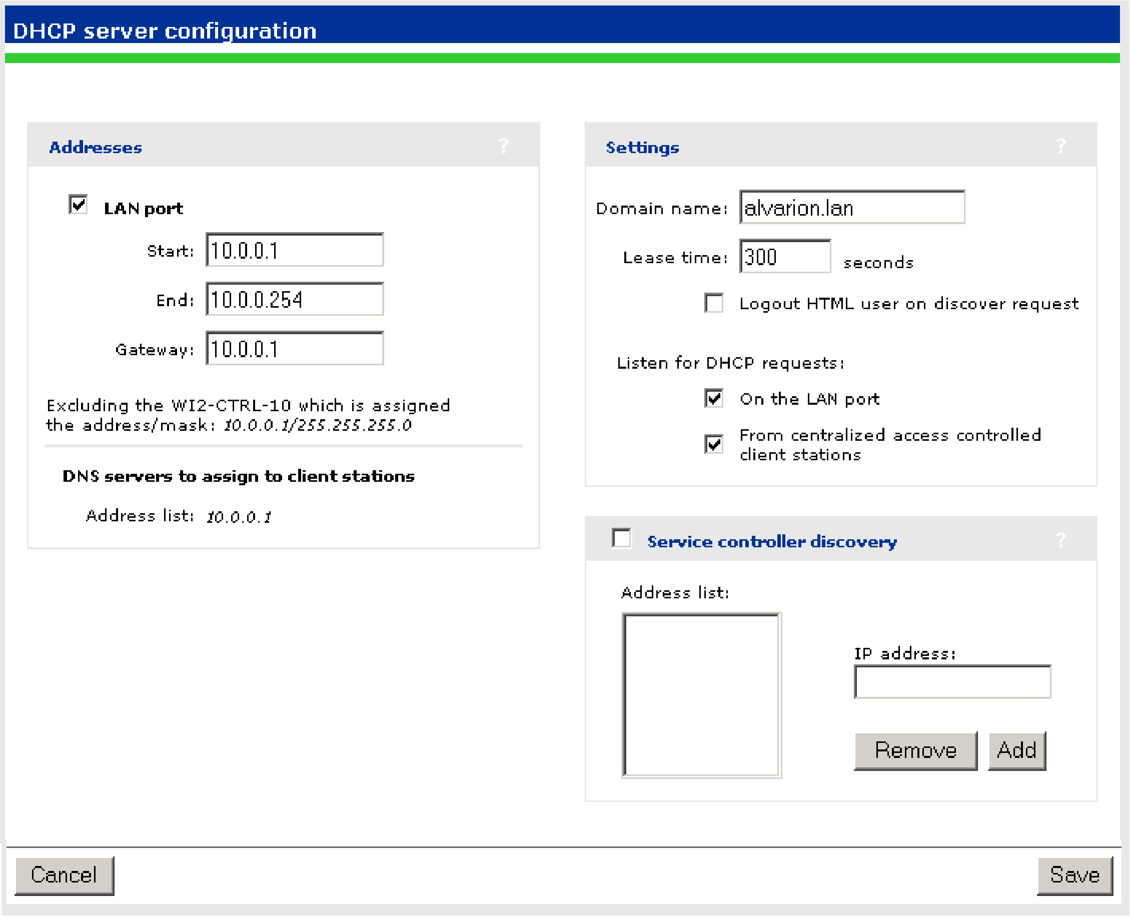
To summarize, this means that by default, any DNS request by a user that matches **wireless.alvarion.com** will return the IP address of the service controller’s Internet port.

7.2.1.1 DHCP Server Configuration

Configure the DHCP server as follows:

1 Select **Service Controller** >> **Network** > **Address allocation.**

2 Select **DHCP server** and then **Configure**.



DHCP server configuration

Addresses

☑ LAN port

Start: 10.0.0.1

End: 10.0.0.254

Gateway: 10.0.0.1

Excluding the WI2-CTRL-10 which is assigned the address/mask: *10.0.0.1/255.255.255.0*

DNS servers to assign to client stations

Address list: *10.0.0.1*

Settings

Domain name: alvarion.lan

Lease time: 300 seconds

☐ Logout HTML user on discover request

Listen for DHCP requests:

☑ On the LAN port

☑ From centralized access controlled client stations

☐ Service controller discovery

Address list:

IP address:

Figure 7-5: DHCP Server Configuration

3. Set the IP address of the default **Gateway** for the service controller to assign to DHCP users. You can usually specify the IP address of the service controller LAN port as the **Gateway.**

NOTE

DNS servers to assign to client stations shows the IP addresses of the DNS servers that the service controller can assign to users. You can define DNS options by selecting **Network > DNS.**

4. Adjust **Domain name** if desired. Specify the domain name for the service controller to return to users. Typically, this will be your corporate domain name.
5. Adjust **Lease time** if desired. Specify the number of seconds of lease time for the service controller to assign to all assigned addresses. Default is 300 seconds.
6. Consider enabling **Logout HTML user on discovery request** when multiple users on your network share the same device. This causes the service controller to log out a device if a DHCP discovery request is received from the device while a DHCP address lease is currently assigned. Otherwise, If a user forgets to log out before turning off the device, the next user will have to wait until the lease expires before being able to log in.
7. For **Listen for DHCP requests**, select the interfaces on which the service controller will listen for DHCP requests.
8. Select **Save**.

NOTE

Even when the service controller DHCP server is active, users can still connect using static IP addresses assigned on different subnets. To configure this feature, select **Public access > Access control** and under **Client options**, select **Allow any IP address**.

7.2.2 DHCP Relay Agent

The service controller provides a flexible DHCP relay implementation. It can listen for requests on the LAN port and forward them to:

- the Internet port
- an IPSec tunnel operating on the Internet port
- a GRE tunnel

Use the following guidelines when configuring DHCP relay:

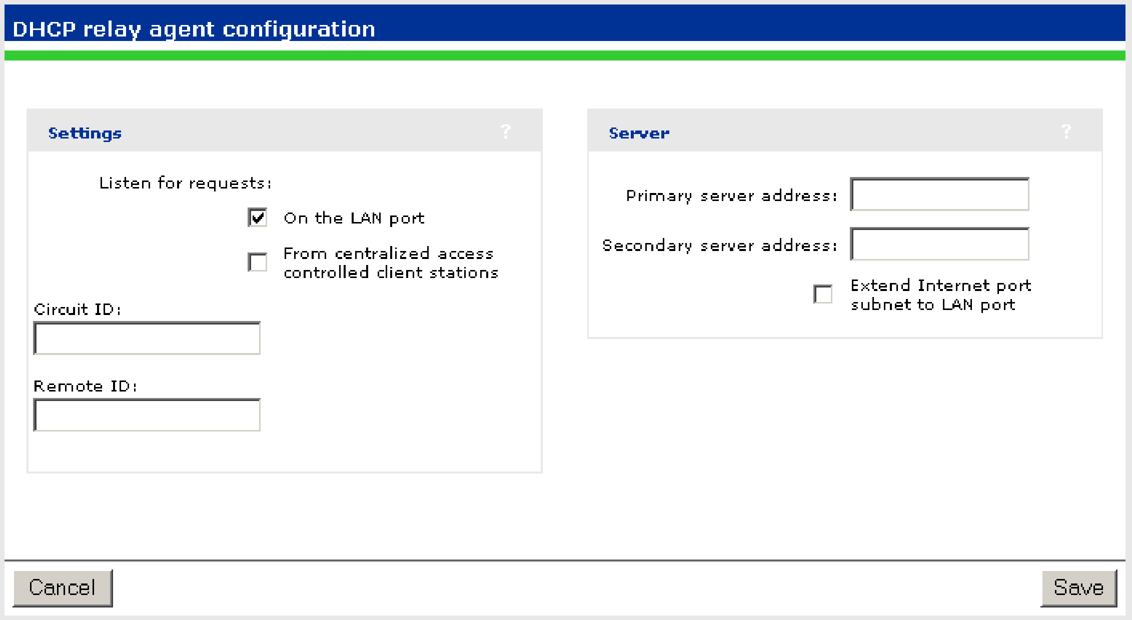
- Routes must be defined on the DHCP servers so that they can successfully send DHCP packets back to the DHCP relay agent running on the service controller. These routes must identify the segment assigned to the service controller's LAN port.
- External DHCP servers must be reachable through one of the service controller's ports.
- DHCP relay is not supported when PPPoE is enabled on the Internet port.
- DHCP relay cannot work if the internal firewall is set to High and NAT is enabled on the Internet port. The DHCP server must be able to ping the assigned address to prevent duplicate assignments.

A separate DHCP relay agent can also be enabled on each virtual network. For details, see “DHCP Relay Agent” on page 118.

7.2.2.1 DHCP Relay Agent Configuration

Configure the DHCP relay agent as follows:

1. Select **Service Controller** >> **Network** > **Address allocation**.
2. Select **DHCP relay agent** and then **Configure**.



DHCP relay agent configuration

Settings

Listen for requests:

☑ On the LAN port

□ From centralized access controlled client stations

Circuit ID:

Remote ID:

Server

Primary server address:

Secondary server address:

□ Extend Internet port subnet to LAN port

Figure 7-6: DHCP Relay Agent Configuration

3 Under **Settings,** select the port on which the service controller listens for DHCP requests, as follows:

- **LAN port**: Listens to any requests from the local network and relays them to the remote DHCP server.

- **From centralized access controlled client stations:** Select this option when centralized access mode is enabled, and you only want to handle requests from wireless users on controlled APs. For more information, see Add xref to section that explains this concept (enabled on the Configuration > Access control page)"Centralized Access Control" on page 102.

- **Circuit ID:** Use this field to attach information to the DHCP request that enables the server to identify the client station that issued the DHCP request. To have the service controller insert dynamic values, use the following placeholders:

  - %S: SSID the client station is associated with.
  - %B: The BSSID the client station is associated with.
  - %V: The VLAN the client station is mapped to.

- **Remote ID:** This field lets you attach information to the DHCP request which lets the server identify the service controller. To have the service controller insert dynamic values, use the following placeholders:
  - %S: SSID the client station is associated with.
  - %B: The BSSID the client station is associated with.
  - %V: The VLAN the client station is mapped to.

4 Under **Server,** configure the following parameters:

- **Primary DHCP server address**: Specify the IP address of the first DHCP server to which the service controller should forward DHCP requests.
- **Secondary DHCP server address**: Specify the IP address of the backup DHCP server to which the service controller should forward DHCP requests.
- **Extend Internet subnet to LAN port**: Used to assign public IPs to specific clients on the LAN port. When enabled, the service controller will alter the DHCP address requests from users so that they appear to originate from the network assigned to the Internet port on the service controller. This will cause the DHCP server to assign IP addresses on this network to all users. The service controller handles all mapping between the two subnets internally.

7.3 VLAN Support

NOTE

This section discusses VLAN configuration on the service controller. To define VLANs on a controlled AP, see "Defining VLANs" on page 73.

The service controller provides a robust and flexible virtual local area network (VLAN) implementation that supports a wide variety of scenarios. For example, VLANs can be used for virtual network ingress and egress mappings to isolate management from user traffic.

Egress VLANS can also be assigned on a per-user basis by setting the appropriate RADIUS attributes in a user's account.

Up to 80 VLAN definitions can be created on the service controller. VLAN ranges are supported enabling a single definition to span a range of VLAN IDs.

The following service controller features can be supported on a VLAN:

- Network address translation (*However, static NAT mappings are not supported.)*
- Management tool access
- SNMP access
- SOAP access
- VPN traffic

For specific examples of how to work with VLANs, see the *Deployment Guide.*

7.3.1 Types of VLANs

The service controller supports three types of VLANs: virtual network-based VLANs, general VLANs, and user-assigned VLANs.

7.3.1.1 Virtual network-based VLANs

Virtual network-based VLANs are VLANs that are assigned to a virtual network profile, either to an ingress or egress mapping.

- To be used as a VSC ingress, a VLAN **must not have** an IP address assigned to it.
- To be used as a VSC egress, a VLAN **must have** an IP address assigned to it.

NOTE

VLANs assigned in a virtual network definition apply to the service controller only. On controlled APs, egress VLAN assignment for a virtual network is done when the virtual network is bound to the AP. For more information, refer to "Defining VLANs" on page 73.

7.3.1.2 General VLANs

General VLANs are VLANs that are not assigned to a VSC profile, which means that:

- Access control does not apply to traffic on these VLANs.
- An address must be assigned to the VLAN either via DHCP or static assignment.
- VLAN traffic is routed.

7.3.1.3 User-assigned VLANs

VLANs can be assigned on a per-user basis by defining the appropriate RADIUS attributes in a user's account (see the *Network Access Admin Guide*), or by setting a VLAN ID in the local user accounts (see "Defining Account Profiles" on page 270).

- Only supported for 802.1X users.
- The VLAN applies only on the controlled AP and not on the service controller.

NOTE

User-assigned VLANs override VLANs assigned by a virtual network on the autonomous AP.

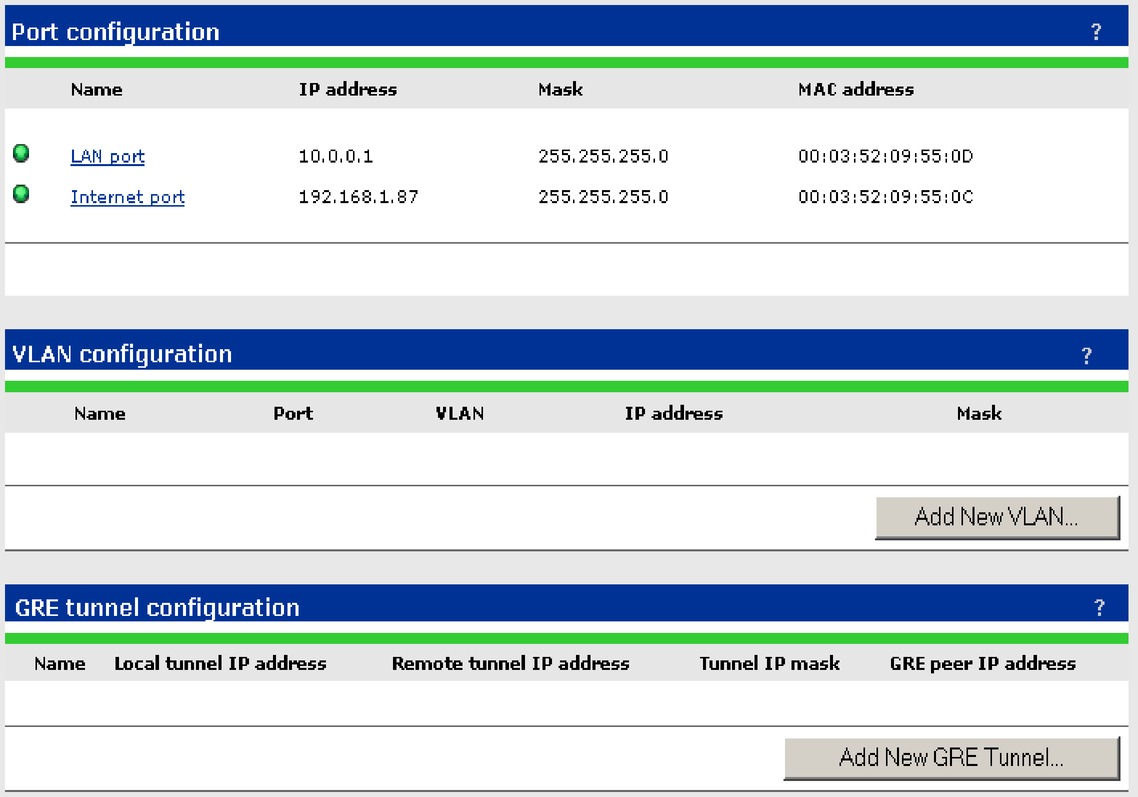
NEED TO ADD AN EXAMPLE HERE: user assigned a VLAN of 20, AP is bound to virtual network with VLAN 30, so user traffic ends up on VLAN 20. On the service controller, VLAN 20 is mapped to a virtual network with egress 40. So, user traffic ends up on VLAN 40.

7.3.1.4 VLAN Ranges

A VLAN assigned to the LAN port can be defined to cover a range of IDs (1 to 4094). This enables a single VLAN definition to accept traffic for one or more VLAN IDs, making it easy to manage a large number of contiguously assigned VLANs. You can use a VLAN range to aggregate traffic from several VLANs and assign it to the same VSC ingress. An IP address cannot be assigned to a VLAN range.

7.3.2 VLAN Configuration

To view and configure VLAN definitions, select **Service Controller** >> **Network** > **Ports**. Initially, no VLANs are defined.



Port configuration ?

	Name	IP address	Mask	MAC address
●	LAN port	10.0.0.1	255.255.255.0	00:03:52:09:55:0D
●	Internet port	192.168.1.87	255.255.255.0	00:03:52:09:55:0C

VLAN configuration ?

Name	Port	VLAN	IP address	Mask

GRE tunnel configuration ?

Name	Local tunnel IP address	Remote tunnel IP address	Tunnel IP mask	GRE peer IP address

Figure 7-7: VLAN Configuration

To add a VLAN, select **Add New VLAN.** The **Add/Edit VLAN** page opens.

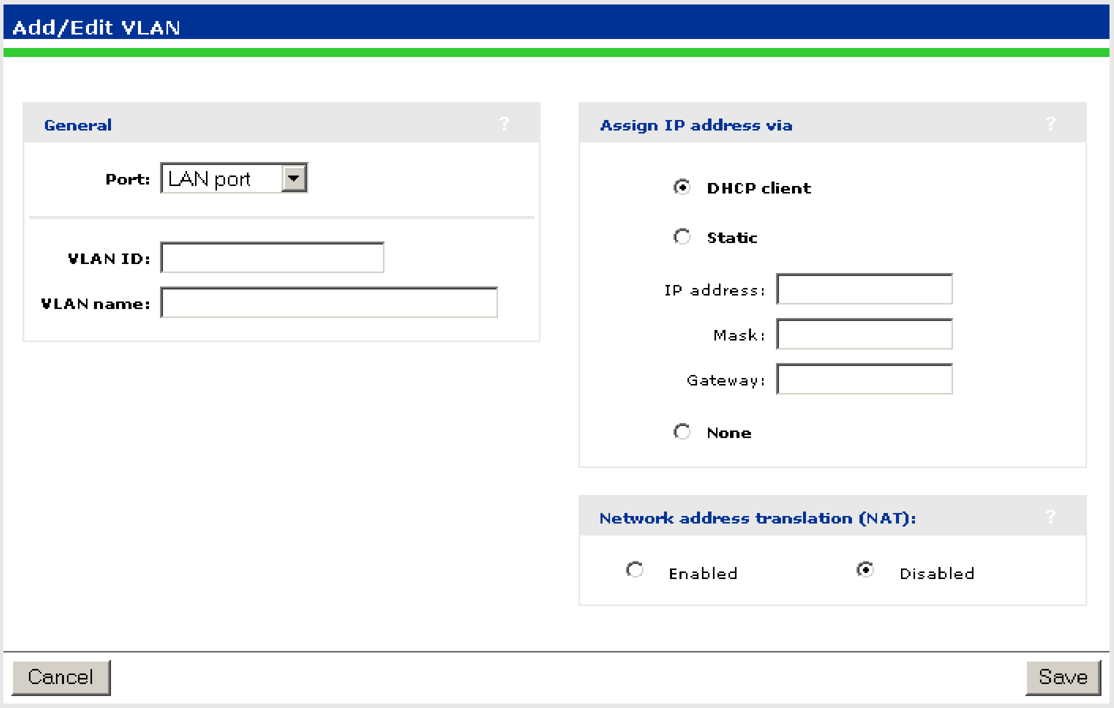


Figure 7-8: Adding a New VLAN

Define VLAN settings as described in the following sections.

7.3.2.1 General

- **Port**: Select the physical interface with which the VLAN is associated. You can define a VLAN on the **Internet port** or **LAN port.**

- **VLAN ID**: Specify an 802.1Q identifier for the VLAN.

If the VLAN is assigned to the LAN port, you can also define a range of VLANs in the form *X-Y*, where *X* and *Y* can be 1 to 4094; for example, *50-60.* This enables a single VLAN definition to accept traffic for one or more VLAN IDs, making it easy to manage a large number of contiguously assigned VLANs. You can define more than one VLAN range, but each range must be distinct and contiguous.

NOTE

VLANS with ranges cannot be used for **VSC egress mapping** and cannot be assigned an IP address.

- **VLAN name**: Specify a name to identify the VLAN definition on the service controller. This name has no operational significance.

7.3.2.2 Assigning an IP address

Specify how the VLAN obtains an IP address, as follows:

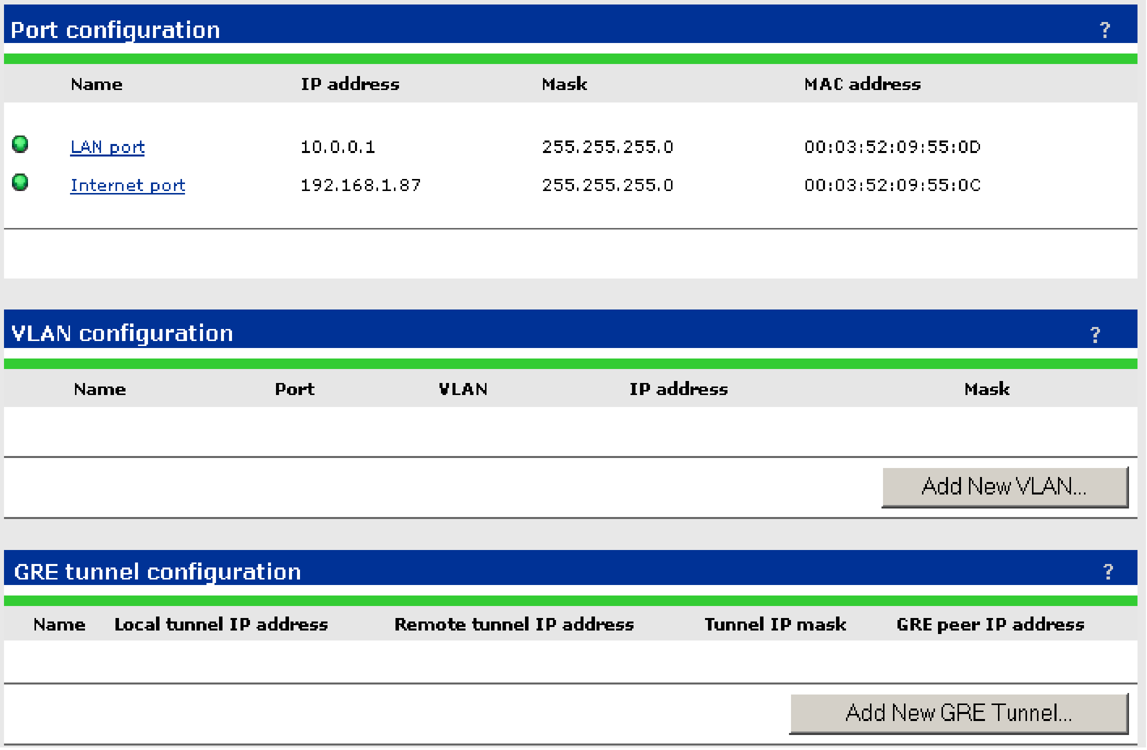
- **DHCP client**: The VLAN obtains its IP address from a DHCP server on the same VLAN.
- There is no support for obtaining a default gateway from the DHCP server.
- **Static**: Enables you to manually assign an IP address to the VLAN. If you select this option, you must specify a static **IP address, Mask,** and **Gateway.**
- **None**: Specifies that this VLAN has no IP address, so that you can use the VLAN for a VSC ingress mapping.

7.3.2.3 NAT

Available only if addressing is **DHCP client** or **Static.** Specify whether network address translation (NAT) is enabled on the VLAN. By default NAT is disabled**.** For more information, see "Network Address Translation (NAT)" on page 181.

7.4 GRE Tunnels

To view and configure GRE tunnel definitions, select **Service Controller** >> **Network** > **Ports**. Initially, no GRE tunnels are defined.



Port configuration ?

	Name	IP address	Mask	MAC address
●	LAN port	10.0.0.1	255.255.255.0	00:03:52:09:55:0D
●	Internet port	192.168.1.87	255.255.255.0	00:03:52:09:55:0C

VLAN configuration ?

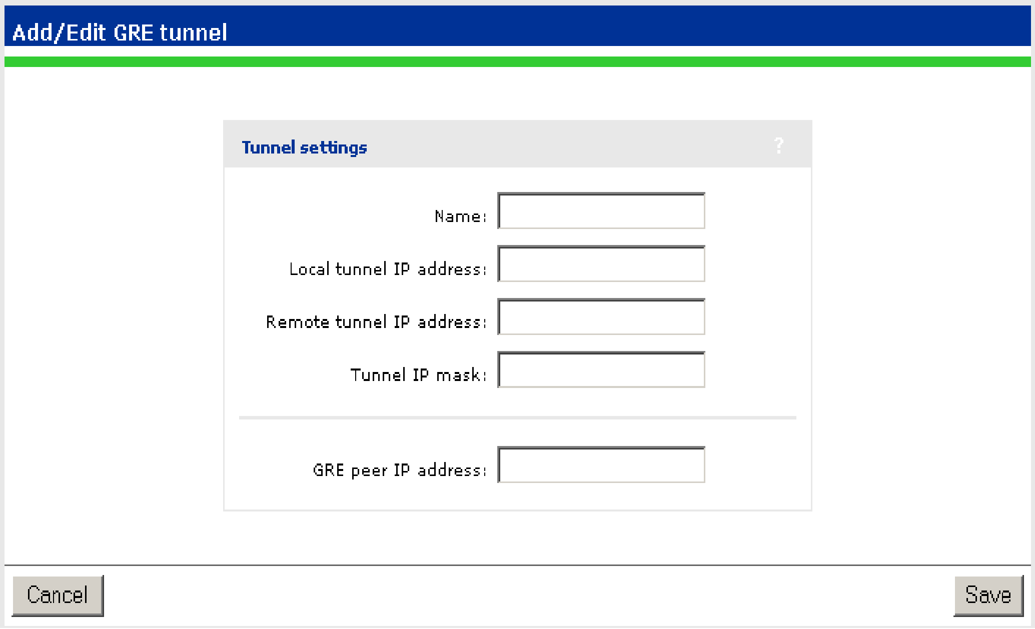
Name	Port	VLAN	IP address	Mask

GRE tunnel configuration ?

Name	Local tunnel IP address	Remote tunnel IP address	Tunnel IP mask	GRE peer IP address

Figure 7-9: GRE Tunnels

To add a GRE tunnel**,** select **Add New GRE Tunnel.** The **Add/Edit GRE Tunnel** page opens.



Add/Edit GRE tunnel

Tunnel settings

Name:	
Local tunnel IP address:	
Remote tunnel IP address:	
Tunnel IP mask:	
GRE peer IP address:	

Figure 7-10: Adding a New GRE Tunnel

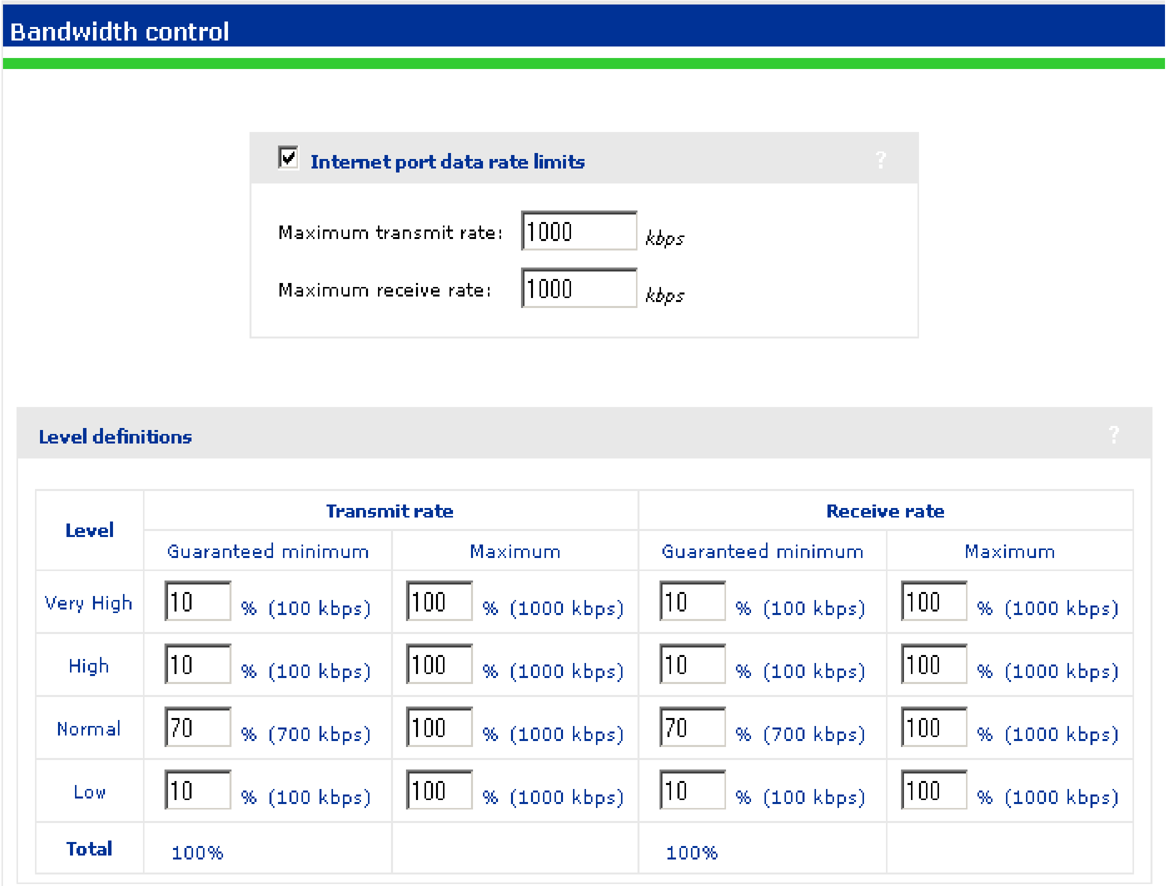
Define tunnel settings as follows.

- **Name:** Tunnel name.
- **Local tunnel IP address:** Specify the IP address of the service controller inside the tunnel.
- **Remote tunnel IP address:** Specify the IP address of the remote device inside the tunnel.
- **Tunnel IP mask:** Specify the mask associated with the IP addresses inside the tunnel.
- **GRE peer IP address:** Specify the IP address of the remote device that terminates the tunnel.

7.5 Bandwidth Control

The service controller incorporates a powerful bandwidth management feature that enables comprehensive control of all user traffic flowing through the service controller.

To configure Bandwidth management, select **Service Controller >> Network > Bandwidth Control.**



Bandwidth control

☑ Internet port data rate limits

Maximum transmit rate: 1000 kbps

Maximum receive rate: 1000 kbps

Level definitions

Level	Transmit rate		Receive rate	
	Guaranteed minimum	Maximum	Guaranteed minimum	Maximum
Very High	10 % (100 kbps)	100 % (1000 kbps)	10 % (100 kbps)	100 % (1000 kbps)
High	10 % (100 kbps)	100 % (1000 kbps)	10 % (100 kbps)	100 % (1000 kbps)
Normal	70 % (700 kbps)	100 % (1000 kbps)	70 % (700 kbps)	100 % (1000 kbps)
Low	10 % (100 kbps)	100 % (1000 kbps)	10 % (100 kbps)	100 % (1000 kbps)
Total	100%		100%	

Figure 7-11: Bandwidth Control

Bandwidth control has two separate components: Internet port data rate limits and bandwidth levels. They interact with the data stream as follows:

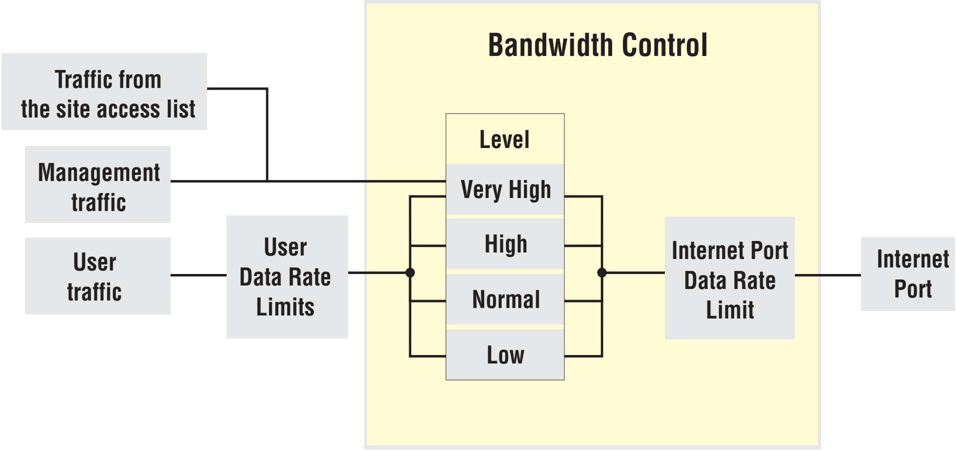


Figure 7-12: Interaction of Bandwidth Control Components with the Data Stream

7.5.1 Internet Port Data Rate Limits

These settings enable you to limit the total incoming or outgoing data rate on the Internet port. If traffic exceeds the rate you set for short bursts, it is buffered. Long overages will result in data being dropped.

To utilize the full available bandwidth, the Maximum transmit rate and Maximum receive rate should be set to match the incoming and outgoing data rates supported by the connection established on the Internet port.

7.5.2 Bandwidth Levels

The service controller provides four levels of traffic priority that you can use to manage traffic flow: *Very High, High, Normal,* and *Low*. The settings for each level are customizable, allowing performance to be tailored to meet a wide variety of scenarios.

7.5.2.1 Assigning Traffic to a Bandwidth Level

Traffic is assigned to a bandwidth level for each virtual network or for each user. Each virtual network can be configured to handle user traffic at a specific bandwidth level. This level applies to users who do not have a specific assignment in their RADIUS account.

- Management traffic (which includes RADIUS, SNMP, and administrator sessions) is assigned to bandwidth level Very High and cannot be changed.

- All traffic assigned to a particular bandwidth level shares the allocated bandwidth for that level across all virtual networks. This means that if you have three virtual networks all assigning user traffic to High, all users share the bandwidth allocated to the High level.

7.5.2.2 Customizing Bandwidth Levels

Bandwidth levels are arranged in order of priority from Very High to Low. Priority determines how free bandwidth is allocated once the minimum rate is met for each level. Free bandwidth is always assigned to the higher priority levels first.

Bandwidth rates for each level are defined by taking a percentage of the maximum transmit and receive rates defined for the Internet port. Each bandwidth level has four rate settings:

- Transmit rate - guaranteed minimum: Minimum amount of bandwidth that will be assigned to a level as soon as outgoing traffic is present on the level.
- Transmit rate - maximum: Maximum amount of outgoing bandwidth that can be consumed by the level. Traffic in excess is buffered for short bursts, and dropped for sustained overages.
- Receive rate - guaranteed minimum: Minimum amount of bandwidth that will be assigned to a level as soon as incoming traffic is present on the level.
- Receive rate - maximum: Maximum amount of incoming bandwidth that can be consumed by the level. Traffic in excess is buffered for short bursts, and dropped for sustained overages.

7.5.3 Example

For example, assume that transmit bandwidth is configured as follows:

	Transmit rates	
	Min	**Max**
Very High	20	20
High	40	100
Normal	20	100
Low	20	20

Next, assume the following bandwidth requirement occurs on transmitted user data:

- High requires 70%, which is 30% more than its minimum.
- Normal requires 50%, which is 30% more than its minimum.
- There is no traffic on Very High or Low.

Since both High and Normal require bandwidth in excess of their guaranteed minimum, each is allocated their guaranteed minimum. This leaves 40% of the bandwidth free to be assigned on a priority basis. High has more priority than Normal, so it takes as much bandwidth as needed. In this case it is 30%, which brings High up to 70%. This leaves 10% for Normal, which is not enough. Traffic is buffered for a short period, and then dropped.

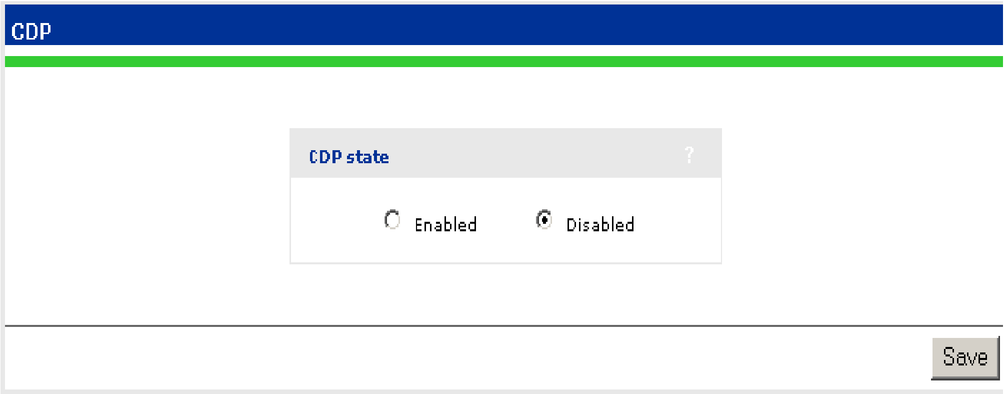
If at the same time Very High traffic is sent, this level immediately steals 20% from the lower levels. In this case, 10% is taken from Normal, returning it to its minimum guaranteed level, and 10% is taken from High.

7.6 CDP

The service controller can be configured to transmit CDP (Cisco Discovery Protocol) information on the LAN port. This information is used to advertise service controller information to third-party devices, such as CDP-aware switches.

The service controller uses CDP information sent by autonomous APs to collect information about these APs for display on the **Management** > **Satellites** page.

To enable CDP transmission, select **Service Controller** >> **Network** > **CDP.**



CDP

CDP state

○ Enabled ● Disabled

Figure 7-13: CDP

NOTE

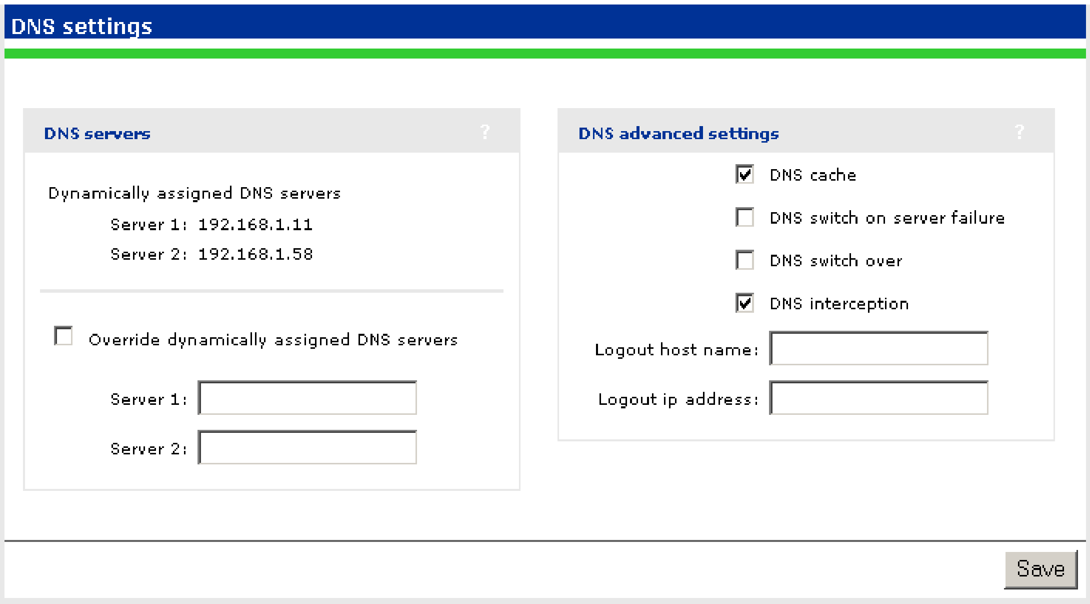
The service controller always listens for CDP information on the LAN port, even when this option is disabled, to build a list of autonomous Alvarion APs. CDP information from third-party devices and controlled Alvarion APs is ignored.

NOTE

Controlled APs always send CDP information.

7.7 DNS

The service controller provides several options to customize DNS handling. To configure these options, select **Service Controller** >> **Network** > **DNS.**



DNS settings

DNS servers

Dynamically assigned DNS servers

Server 1: 192.168.1.11

Server 2: 192.168.1.58

□ Override dynamically assigned DNS servers

Server 1:

Server 2:

DNS advanced settings

☑ DNS cache

□ DNS switch on server failure

□ DNS switch over

☑ DNS interception

Logout host name:

Logout ip address:

Figure 7-14: DNS

7.7.1 DNS Servers

- **Dynamically assigned servers**: Gives information about the DNS servers that are assigned to the service controller. This option does not appear if static addressing is in use.

- **Override dynamically assigned DNS servers**: Enable this checkbox to use the DNS servers that you specify on this page to replace those that are assigned to the service controller. This option does not appear if static addressing is in use.

  - **Server 1**: Specify the IP address of the primary DNS server for the service controller to use.

  - **Server 2**: Specify the IP address of the secondary DNS server for the service controller to use.

NOTE

When using Active Directory, the DNS servers should be the Active Directory servers or the devices that provide SRV records

7.7.2 DNS Advanced Settings

- **DNS cache**: Enable this checkbox to activate the DNS cache. Once a host name is successfully resolved to an IP address by a remote DNS server, it is stored in the cache. This speeds up network performance, because the remote DNS server does not have to be queried for subsequent requests for this host.

An entry stays in the cache until one of the following is true:

- » An error occurs when connecting to the remote host
- » The time to live (TTL) of the DNS request expires
- » The service controller restarts

- **DNS interception**: When enabled, the service controller intercepts all DNS requests and relays them to the configured DNS servers. DNS interception must be enabled to support:

  - » Redirection of users to the public access interface login page when the service controller cannot resolve the domain requested by the user. For example, if the user is using a private or local domain as the default home page in its browser.
  - » Users configured to use HTTP proxy.
  - » Users with static IP addresses when the **Allow any IP address** option is enabled on the **Public access > Access control** page.

When disabled, the service controller does not intercept any DNS requests, enabling devices to use a DNS server other than the service controller. To support this option, you must set **Network > Address allocation** to **DHCP relay agent** or **Static**.

NOTE

When **Network > Address allocation** is set to **DHCP Server** the service controller always returns its own address as the DNS server. Disabling DNS interception in this case causes all DNS requests to fail.

7.8 IP Routes

The routing module on the service controller provides the following features:

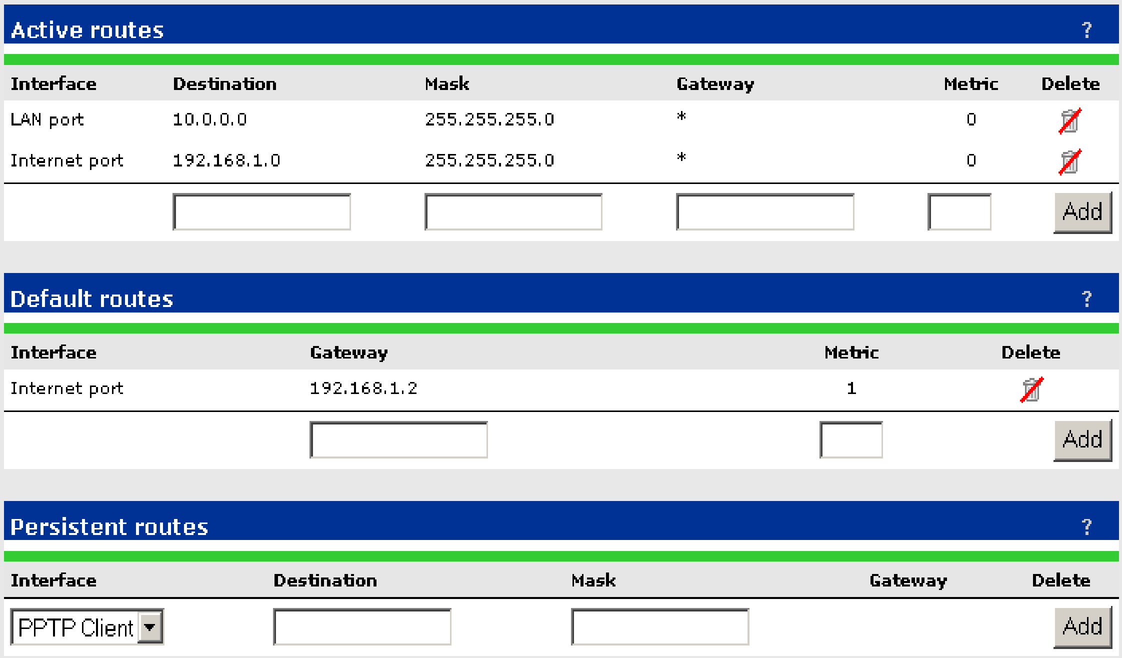
- Compliance with RFC 1812, except for multicast routing
- Supports Classless Inter Domain Routing (CIDR)
- Supports Routing Internet Protocol (RIP) versions 1 and 2 in active or passive mode

Output from the router is sent to the appropriate logical interface based on the target address of the traffic. Supported logical interfaces include:

- VLAN
- Untagged
- IPSec client
- PPTP client
- GRE tunnel

7.8.1 Configuration

To view and configure IP routes, select **Service Controller** >> **Network** > **IP routes**.



Active routes ?

Interface	Destination	Mask	Gateway	Metric	Delete
LAN port	10.0.0.0	255.255.255.0	*	0	🗑
Internet port	192.168.1.0	255.255.255.0	*	0	🗑
					Add

Default routes ?

Interface	Gateway	Metric	Delete
Internet port	192.168.1.2	1	🗑
			Add

Persistent routes ?

Interface	Destination	Mask	Gateway	Delete
PPTP Client ▾				Add

Figure 7-15: Configuration of IP Routes

7.8.1.1 Active Routes

This table shows all active routes on the service controller. You can add routes by specifying the appropriate parameters and then selecting **Add.**

The routing table is dynamic and is updated as needed. This means that during normal operation the service controller adds routes to the table as required. You cannot delete these system routes.

The following information is shown for each active route:

- **Interface**: The port through which traffic is routed. When you add a route, the service controller automatically determines the interface to be used based on the **Gateway** address.
- **Destination**: Traffic addressed to this IP address is routed.
- **Mask**: Number of bits in the destination address that are checked for a match.
- **Gateway**: IP address of the gateway to which the service controller forwards routed traffic (known as the next hop).

An asterisk is used by system routes to indicate a directly connected network.

Routes cannot be manually specified for IPSec. These routes are automatically added by the system based on the settings for the IPSec security association.

- **Metric**: Priority of a route. If two routes exist for a destination address, the service controller chooses the one with the lower metric.

7.8.1.2 Default Routes

The **Default routes** table shows all default routes on the service controller. Default routes are used when traffic does not match any route in the Active routes table. You can add routes by specifying the appropriate parameters and then selecting **Add.**

The routing table is dynamic and is updated as needed. If more than one default route exists, the first route in the table is used.

The following information is shown for each default route:

- **Interface**: The port through which traffic is routed. When you add a route, the service controller automatically determines the interface to be used based on the **Gateway** address.
- **Gateway**: IP address of the gateway to which the service controller forwards routed traffic (known as the next hop).
- An asterisk is used by system routes to indicate a directly connected network.
- **Metric**: Priority of a route. If two routes exist for a destination address, the service controller chooses the one with the lower metric.

7.8.1.3 Persistent Routes

Persistent routes are automatically deleted and then restored each time the interface they are associated with is closed and opened. When the routes are active, they also appear in the Active routes table.

7.8.1.4 PPTP Client

The service controller provides an **Auto-route discovery** option to enable it to automatically discover and add routes for IP addresses on the other side of a Point-to-Point Tunnelling Protocol (PPTP) tunnel. The addresses must be part of the remote domain as specified on the **Security > PPTP client** page. Routes are added only when an attempt is made to access the target addresses.

7.8.1.4.1 About PPTP Client Routes (Internet Port)

If you disabled the **Auto-route discovery** option (**Security > PPTP client**), or if you need to access IP addresses that are not part of the specified domain, you must define the appropriate persistent routes.

7.8.1.4.2 About PPTP Server Routes (Internet Port)

Activation of the route can be triggered by a specific username. When a user establishes a connection with the service controller’s PPTP server, its username is checked against the persistent routes list and if a match is found, the route is enabled.

7.9 Network Address Translation (NAT)

Network address translation is an address mapping service that enables one set of IP addresses to be used on an internal network, and a second set to be used on an external network. NAT handles the mapping between the two sets of addresses.

Generally NAT is used to map all addresses on an internal network to a single address for use on an external network like the Internet. The main benefits are that NAT:

- Enables several devices to share a single connection
- Effectively hides from the outside network the IP addresses of all devices on the internal network.

This is illustrated as follows:

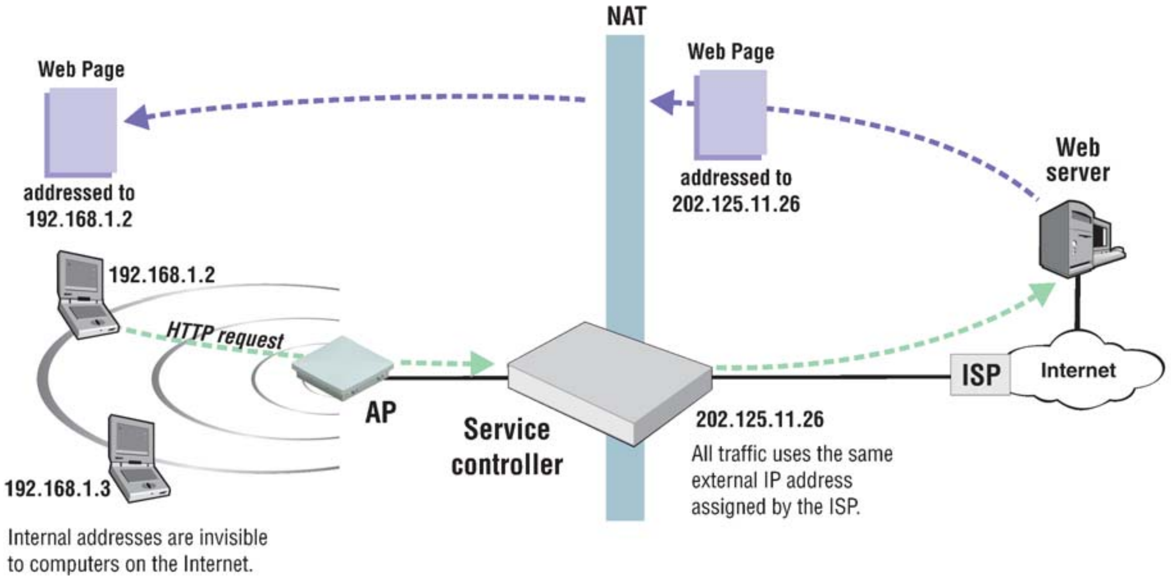


Figure 7-16: Network Address Translation

NAT can be useful in conjunction with virtual private network (VPN) connections. When two networks are connected through a VPN tunnel, it may be desirable to obscure the address of local computers for security reasons.

7.9.1 NAT Security and Static Mappings

One of the benefits of NAT is that it effectively hides the IP addresses of all computers on the internal network from the outside network. In some cases, however, it is useful to make a computer on the internal network accessible externally. For example, a Web server or FTP server.

Static NAT mapping addresses this problem. Static NAT mapping enables you to route specific incoming traffic to an IP address on the internal network. For example, to support a Web server, you can define a static NAT mapping to route traffic on TCP port 80 to an internal computer running a web server.

A static NAT mapping allows only one internal IP address to act as the destination for a particular protocol (unless you map the protocol to a nonstandard port). For example, you can run only one Web server on the internal network.

CAUTION

If you use a NAT static mapping to enable a secure (HTTPS) web server on the internal network on TCP port 443, remote access to the management tool is no longer possible, as all incoming HTTPS requests are routed to the internal web server and not to the management tool. You can change the default management port (TCP 443) to an alternate unused TCP port in this case.

NOTE

If you create a static mapping, the firewall is automatically opened to accept the traffic. However, this firewall rule is not visible on the Firewall configuration page.

The following table indicates how some common applications are affected by NAT.

Application	NAT
FTP (passive mode)	Requires a static mapping to function.
FTP (active mode)	Requires a static mapping to function.
NetMeeting	Requires a static mapping to function.
Telnet	Requires a static mapping to function.
Windows networking	No effect

The service controller provides pre-configured static mappings for most common applications, which you can enable as needed.

Most web browsers use FTP in active mode. Some browsers provide a configuration option that enables you to alter this. Use the following steps to change this behavior in Microsoft Internet Explorer.

1 Select **Tools > Internet options** to open the **Internet options** dialog.

2 Select the **Advanced** tab.

3 Under **Browsing,** enable the **Use Passive FTP for compatibility with some firewalls and DSL modems** checkbox.

7.9.1.1 NAT Example

The following example shows you how to configure static NAT mappings to run a web server and an FTP server on the internal network. This scenario might occur if you use the service controller in an enterprise environment.

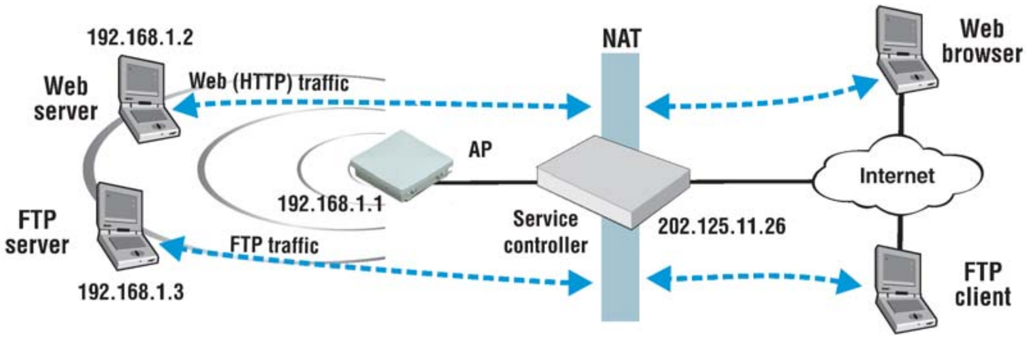


Figure 7-17: NAT Example

By creating static NAT mappings, FTP and HTTP (Web) traffic can be routed to the proper user. Note that the addresses of these stations are still not visible externally. Remote computers send their requests to 202.125.11.26, and the service controller routes them to the proper client.

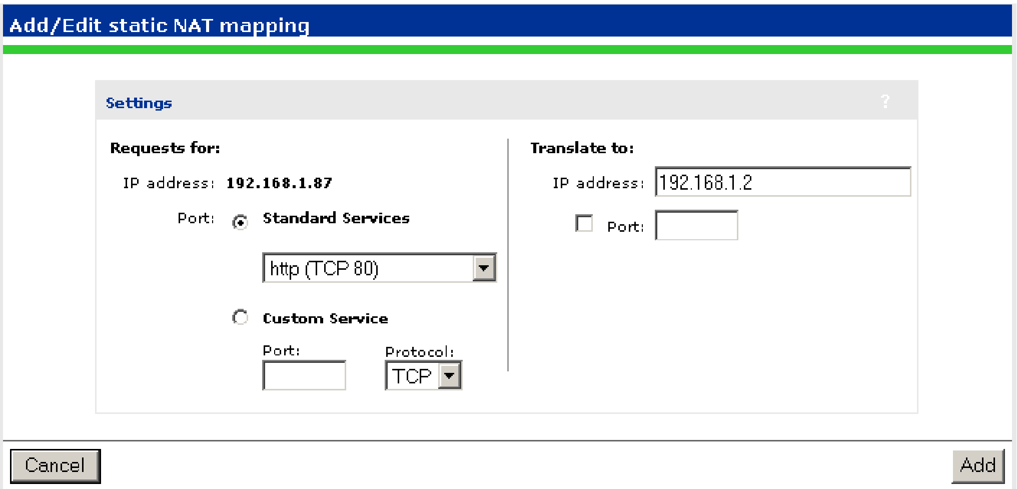
Use the following steps to configure the service controller to support this example.

1 Select **Service Controller** >> **Network** > **NAT** > **Add New Static NAT Mapping**.

2 On the NAT mappings page, select **Add New Static NAT Mapping**.

3 Under **Requests for**, select **Standard Services**, and then select **http (TCP 80).**

4 Under **Translate to**, specify the IP address of the Web server, for example **192.168.1.2.** The Settings box should now look similar to this:



Add/Edit static NAT mapping

Settings

Requests for:

IP address: 192.168.1.87

Port: ● Standard Services

http (TCP 80)

○ Custom Service

Port:

Protocol: TCP

Translate to:

IP address: 192.168.1.2

□ Port:

Figure 7-18: Add/Edit Static NAT Mapping

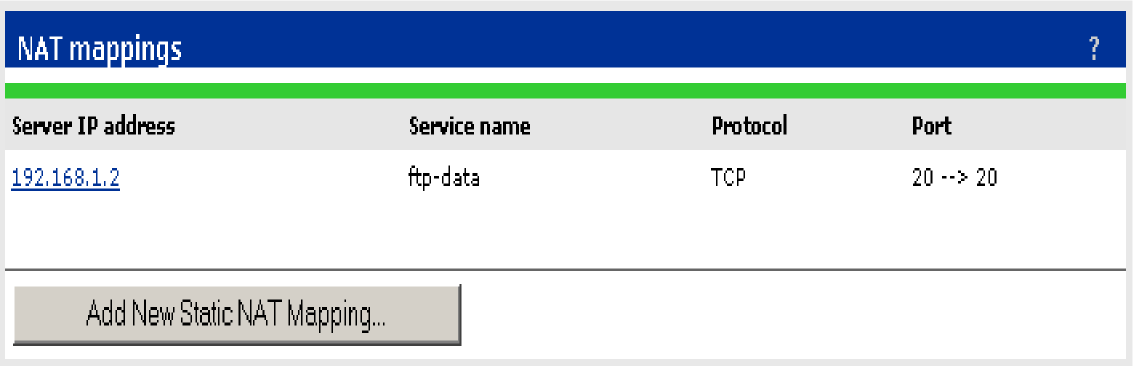
5 Select **Add** to save your changes and return to the NAT mappings page. The new mapping is added to the table.

6 To support the FTP server, create two additional mappings with the following values:

» Set **Standard Services** to **ftp-data (TCP 20)** and set **IP address** to **192.168.1.3**.

» Set **Standard Services** to **ftp-control (TCP 21)** and set **IP address** to **192.168.1.3**.

The NAT mappings table should now show all three mappings:



NAT mappings

Server IP address	Service name	Protocol	Port
192.168.1.2	ftp-data	TCP	20 --> 20

Figure 7-19: NAT Mapping Table

7.9.2 One-to-one NAT

NOTE

This feature only applies to VPN traffic using PPTP on the Internet port.

In its default configuration, NAT translates all internal IP address to a single external IP address. As a result, all user sessions to an external resource appear to originate from the same IP address. Certain applications do not allow multiple connections from the same IP address, or impose a limit. For example, some PPTP servers require a unique IP address for each user.

One-to-one NAT addresses this problem. One-to-one NAT enables you to assign multiple IP addresses to the Internet port and to use those addresses to distinguish outgoing NAT traffic for users making PPTP connections.

One-to-one NAT functions as follows:

- Define alternate static addresses for the Internet port. These addresses must be valid on the Internet.
- Define the `one-to-one-nat` attribute in the account for each user that requires a unique IP address. Or define the `default-user-one-to-one-nat` attribute on the service controller.
- When a user with one-to-one NAT support logs into the public access interface and establishes a PPTP session, the service controller reserves the next available alternate IP address for that user. If all alternate IP addresses are in use, or none has been defined, the default IP address of the Internet port is used.

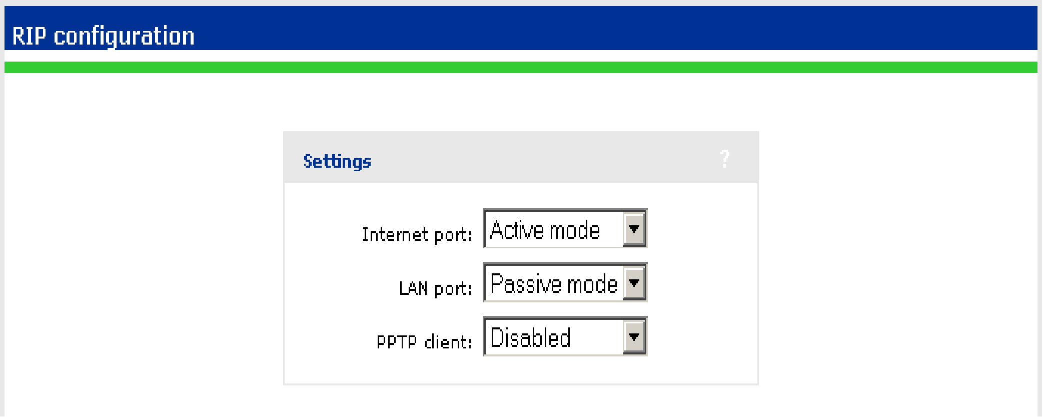
The address is reserved for as long as the user is logged in and using a VPN connection. Therefore, you must define enough alternate IP addresses to support the maximum number of active VPN sessions you expect to have at any one time.

7.10 RIP

The service controller supports Routing Information Protocol (RIP) versions 1 and 2. RIP can operate in one of two modes on the interfaces you select.

- **Passive mode**: The service controller listens for routing broadcasts to update the routing table, but does not broadcast its own routes.
- **Active mode**: The service controller listens for routing broadcasts to update the routing table, and also broadcast its own routes.

For example:



RIP configuration

Settings

Internet port: Active mode

LAN port: Passive mode

PPTP client: Disabled

Figure 7-20: RIP Configuration

NOTE

RIP is not supported if you are using PPPoE on the Internet port.

7.11 IP QoS

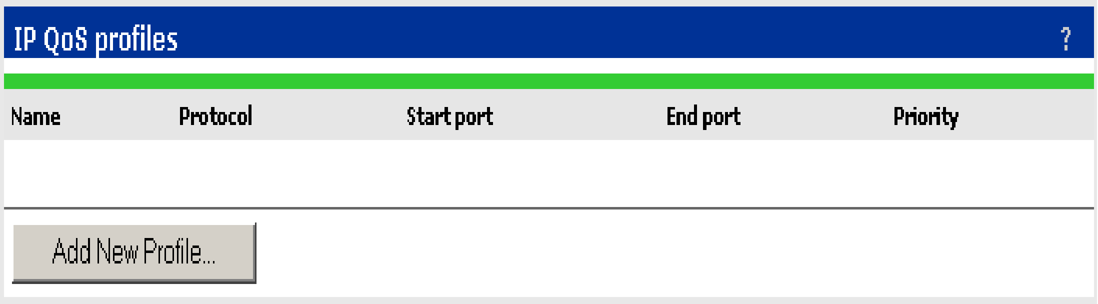
To ensure that critical applications have access to the required amount of wireless bandwidth, you can classify packets destined for the wireless interface into priority queues based on a number of criteria. For example, you can use any of the following to place data packets in one of four priority queues for transmission onto the wireless interface:

- TCP source port
- UDP source port
- Destination port
- Port ranges

You configure IP quality of service (QoS) by creating IP QoS profiles that you can then associate with virtual networks or use for global wireless settings. You can configure as many as 32 IP QoS profiles on the service controller. You can associate as many as 10 IP QoS profiles with each virtual network.

7.11.1 Configuration

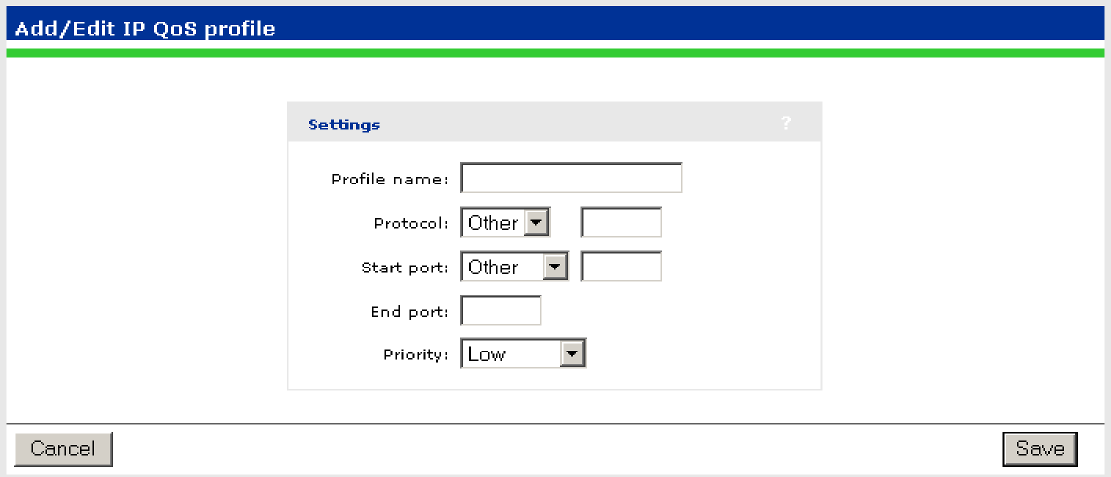
To view and configure IP QoS profiles, select **Service Controller** >> **Network** > **IP QoS**. Initially, no profiles are defined.



Name	Protocol	Start port	End port	Priority

Figure 7-21: IP QoS Profiles

To create an IP QoS profile select **Add New Profile**.



Add/Edit IP QoS profile

Settings

Profile name:

Protocol: Other

Start port: Other

End port:

Priority: Low

Figure 7-22: Creating and IP QoS Profile

7.11.1.1 Settings

- **Profile name:** Specify a unique name to identify the profile.

- **Protocol:** Specify an IP protocol to use to classify traffic by specifying its Internet Assigned Numbers Authority (IANA) protocol number. Protocol numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually. You can find IANA-assigned protocol numbers at http://www.iana.org.

- **Start port/ End port:** Optionally specify the first and last port numbers in the range of ports to which this IP QoS profile applies. To specify a single port, specify the same port number for both **Start port** and **End port.** Port numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually.

NOTE

To accept traffic on all ports for a specified protocol, set **Start port** to **Other** and **0.** Also set **End port** to 65535.

- **Priority:** Select the priority level that will be assigned to traffic that meets the criteria specified in this IP QoS profile.

NOTE

It is strongly recommended that you reserve **Very high** priority for voice applications.

7.11.2 Example

This example shows how to create two IP QoS profiles and associated them with a virtual network. The two profiles are:

- **Voice**: Provides voice traffic with high priority.
- **Web:** Provides HTTP traffic with low priority.

7.11.2.1 Create the Profiles

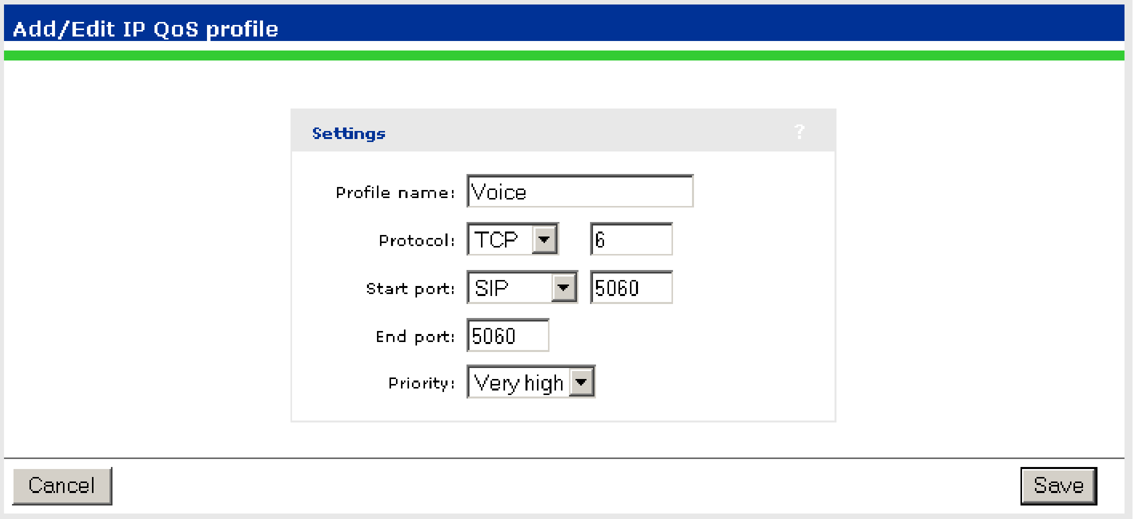
1 Select **Network > IP QoS,** and then **Add New Profile.** The **IP QoS Profile** page opens.

2 Under **Profile name,** specify **Voice.**

3 Under **Protocol,** from the drop-down list select **TCP.**

4 Under **Start port,** from the drop-down list select **SIP. Start port** and **End port** are automatically populated with the correct value: **5060.**

5 Under **Priority,** from the drop-down list select **Very High.**



Profile name: Voice

Protocol: TCP 6

Start port: SIP 5060

End port: 5060

Priority: Very high

Figure 7-23: Creating and IP QoS Profile: Example 1

6 Select **Save.**

NOTE

You could also create another profile using the same parameters but for UDP to cope with any kind of SIP traffic.

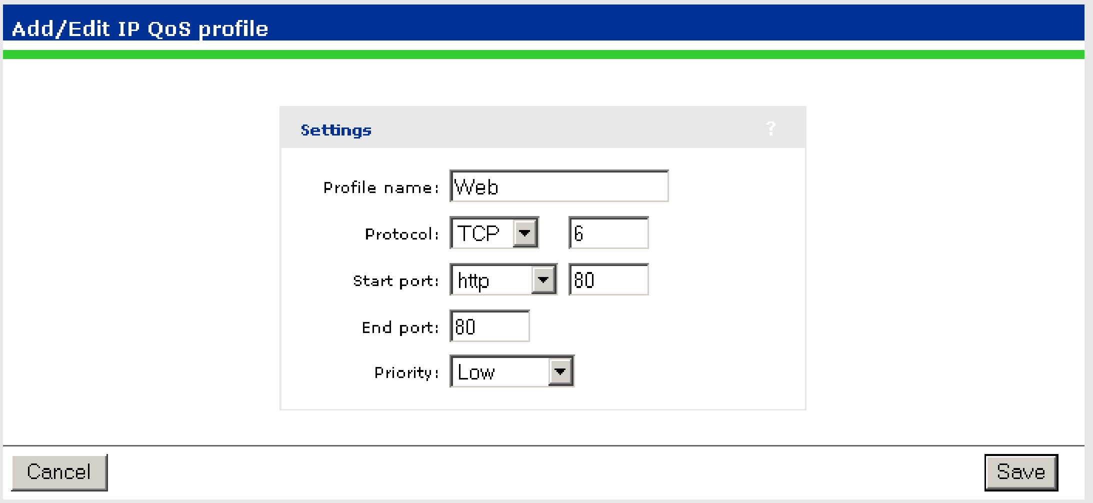
7 On the **IP QoS Profile** page select **Add New Profile.**

8 Under **Profile name,** specify **Web.**

9 Under **Protocol,** from the drop-down list select **TCP.**

10 Under **Start port,** from the drop-down list select **http. Start port** and **End port** are automatically populated with the common HTTP port, **80.**

11 Under **Priority,** from the drop-down list select **Low.**



Add/Edit IP QoS profile

Settings

Profile name: Web

Protocol: TCP 6

Start port: http 80

End port: 80

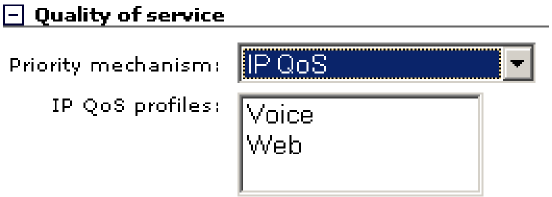
Priority: Low

Figure 7-24: Creating and IP QoS Profile: Example 2

12 Select **Save.**

7.11.2.2 Assign the Profiles to a Virtual Network

1 In the **Network Tree** select **virtual networks** (if not visible, first click the + symbol to the left of **Service Controller**) and then select one of the virtual network profiles in the **Name** column. Scroll down to the **Quality of service** section of the **Virtual AP** box.



Quality of service

Priority mechanism: IP QoS

IP QoS profiles: Voice
Web

Figure 7-25: Quality of Service section of the Virtual AP Box

2 Set **Priority mechanism** to **IP QoS.**

3 in **IP QoS profiles**, Ctrl-click each profile .

4 Select **Save.**

7.12 IGMP Proxy

This feature provides support for multicast routing using IGMP (Internet Group Management Protocol), which is typically required by the service controller. When enabled, IGMP:

- Routes all multicast traffic received on the Upstream interface to the Downstream interface.
- Listens for IGMP host membership reports from authenticated users on the Downstream interface and forwards them to the Upstream interface. IGMP host membership reports from unauthenticated users are ignored.

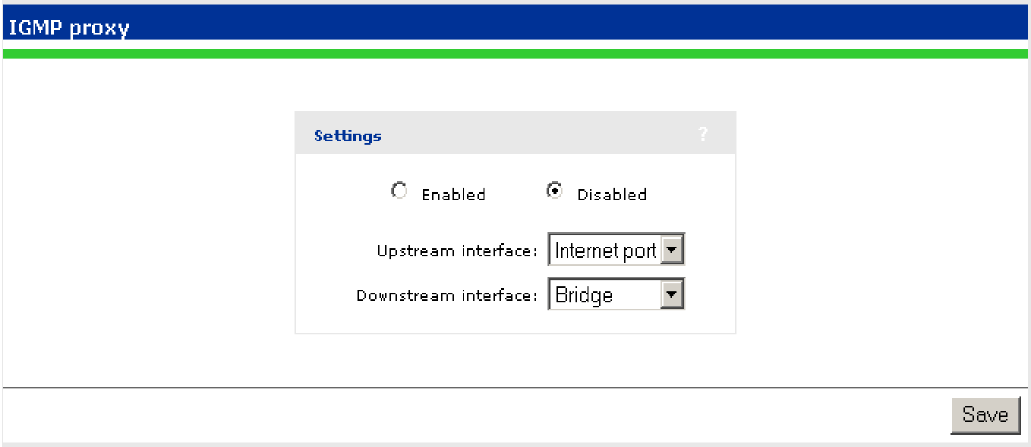
NOTE

An access list definition must be created to accept the multicast traffic (video streams, etc.)

NOTE

Due to the nature of multicast traffic, once a user registers for a stream it automatically becomes visible to unauthenticated users as well. (However, unauthenticated users are not able to register with the IGMP group).

To view and configure IGMP proxy settings, select **Service Controller** >> **Network** > **IGMP proxy**.



IGMP proxy

Settings

○ Enabled ● Disabled

Upstream interface: Internet port

Downstream interface: Bridge

Figure 7-26: IGMP Proxy

8

Chapter 8 - Management

In This Chapter:

8.1 Management Tool

The management tool is a web-based interface to the service controller that provides easy access to all configuration and monitoring functions.

8.1.1 Management Scenarios

For complete flexibility, you can manage the service controller both locally and remotely. The following management scenarios are supported:

- Local management using a computer that is connected to the LAN or Internet port on the service controller. This may be a direct connection or through a switch.

- Remote management via the Internet with or without a VPN connection. See “Creating VPN Connections” on page 236 for more information on using the service controller’s integrated VPN clients to create secure remote connections.

8.1.2 Management Station

The *management station* refers to the computer that an administrator uses to connect to the management tool**.** To act as a management station, a computer must:

- Have a JavaScript-enabled web browser installed (at least Microsoft Internet Explorer 7.0 or Mozilla Firefox 2.0).

- Be able to establish an IP connection with the service controller.

NOTE

Before installation ensure that TCP/IP is installed and configured on the management station. IP addressing can be either static or DHCP. A unique feature of the service controller is its ability to support connections from users that have a preconfigured static IP address.

8.1.3 Starting the Management Tool

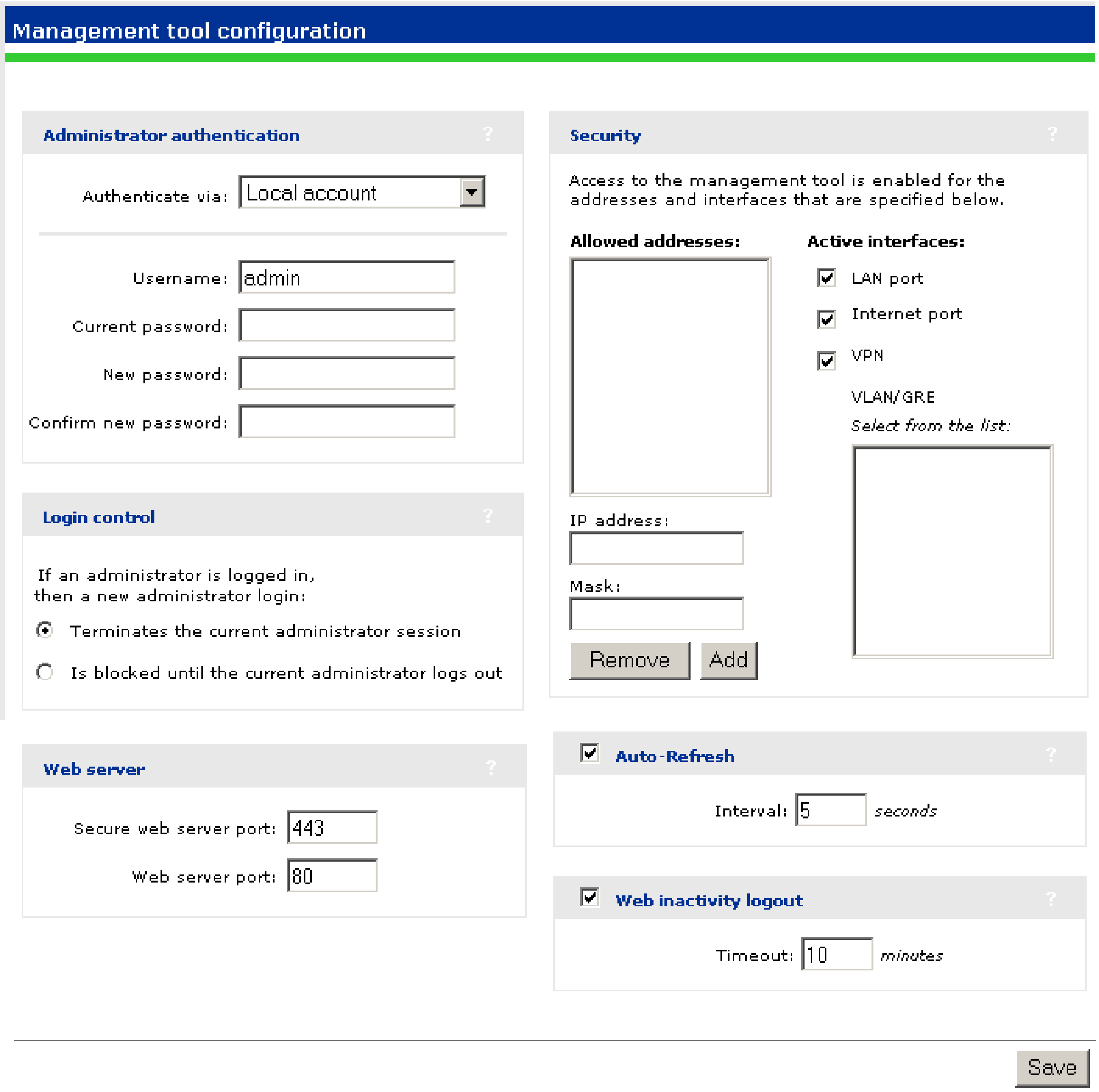
To launch the management tool, specify the following in the address bar of your browser:

```
https://Service_Controller_IP_address
```

By default, the address 192.168.1.1 is assigned to the LAN port. For information on starting the management tool for the first time, see “Configuration Procedure” on page 27.

8.1.4 Customizing Management Tool Settings

To customize management tool settings, select **Service Controller** >> **Management** > **Management tool**.



Management tool configuration

Administrator authentication

Authenticate via: Local account

Username: admin

Current password:

New password:

Confirm new password:

Login control

If an administrator is logged in, then a new administrator login:

● Terminates the current administrator session

○ Is blocked until the current administrator logs out

Web server

Secure web server port: 443

Web server port: 80

Security

Access to the management tool is enabled for the addresses and interfaces that are specified below.

Allowed addresses:

IP address:

Mask:

Active interfaces:

☑ LAN port

☑ Internet port

☑ VPN

VLAN/GRE

Select from the list:

☑ Auto-Refresh

Interval: 5 *seconds*

☑ Web inactivity logout

Timeout: 10 *minutes*

Figure 8-1: Customizing Management Tool Settings

8.1.4.1 Administrator Authentication

Access to the management tool is protected by a username and password. The factory default setting for both is **admin**. It is recommended that you change both at initial setup, and then regularly thereafter.

CAUTION

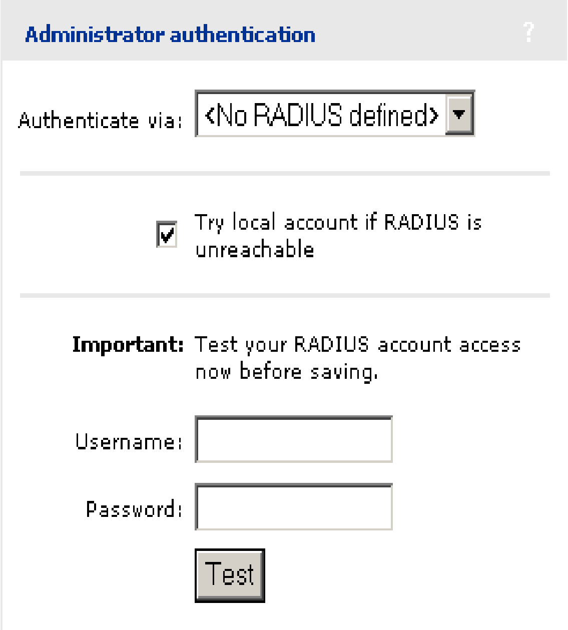
If you forget the administrator password, the only way to access the management tool is to reset the service controller **to factory default settings. For information see** “Resetting to Factory Defaults” on page 359**.**

8.1.4.2 Authenticating Administrators Using a RADIUS Server

The service controller can be configured to use an external RADIUS server to authenticate administrators**.** One advantage of this method is that it enables several administrator accounts to be created, each with its own username and password.

Configure RADIUS authentication as follows:

1. Define an account for the administrator on the RADIUS server.
2. On the service controller, create a RADIUS profile that will connect the service controller to the RADIUS server. See “Configuring a RADIUS Client Profile on the Service Controller” on page 216.
3. Under **Administrator authentication**, set **Authenticate via** to the RADIUS profile you created. In this example, the profile is called **Rad-1**.



Administrator authentication

Authenticate via: <No RADIUS defined>

☑ Try local account if RADIUS is unreachable

Important: Test your RADIUS account access now before saving.

Username:

Password:

Figure 8-2: Authenticating Administrators

4. Enable **Try local account if RADIUS unreachable.** This will allow you to login using the local account if the connection to the RADIUS server is unavailable.
5. It is recommended that before saving, you specify the **Username** and **Password** and select **Test** to ensure that the RADIUS server is reachable and that the administrator account is working properly..

CAUTION

If you do not enable the "Try local account if RADIUS unreachable option" and the service controller is unable to reach the RADIUS server, you will not be able to login.

8.1.5 Login Control

To maintain the integrity of the configuration settings, only one user can be connected to the management tool at a given time. To prevent the management tool from being locked by an idle user, two mechanisms are in place:

- If a user's connection to the management tool remains idle for more than ten minutes, the service controller automatically terminates the user's session. Use the **Web inactivity logout** option to customize this behavior.
- If a second user connects to the management tool and authenticates with the correct username and password, the first user's session terminates. You can change this mechanism to block the login of the second administrator.

- If login to the management tool fails five times in a row (bad username and/or password), login privileges are blocked for five minutes. Once five minutes expires, login privileges are once again enabled. However, if the next login attempt fails, privileges are again suspended for five minutes. This cycle continues until a valid login occurs.

8.1.6 Web Server

You can also configure the web server ports from which access to the management tool is permitted.

- **Secure web server port**: Specify a port number for the service controller to use to provide secure HTTPS access to the management tool**.** Default is 443.

- **Web server port**: Specify a port number for the service controller to use to provide standard HTTP access to the management tool**.** These connections are met with a warning, and the browser is redirected to the secure web server port. Default is 80.

8.1.7 Security

The management tool is protected by the following security features:

- **HTTPS:** Communications between a management station and the service controller is protected using the Secure Hypertext Transport Protocol. Before logging on to the management tool**,** you must accept a security certificate. Because the default certificate provided with the service controller is self-signed by Alvarion Ltd., it will trigger a warning message on most browsers. To remove this warning message, you must replace the default certificate with a valid certificate signed by a certificate authority. See "Managing Certificates" on page 248 for instructions on how to replace the default certificate.

- **Port blocking:** You can enable or disable access to the management tool for each of the following:

  - LAN port
  - Internet port
  - VPN
  - VLAN

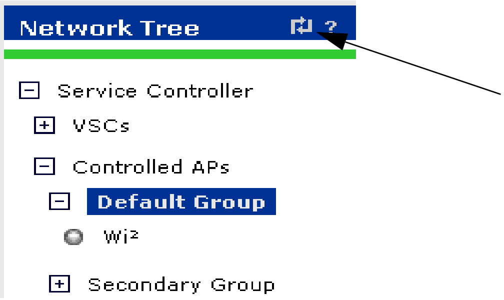
» GRE

These settings also apply when SSH is used to access the command line interface.

- **Allowed IP address:** You can configure a list of subnets from which access to the management tool is permitted.

8.1.8 Auto-refresh

This option controls how often the service controller updates the information in group boxes that show the auto-refresh icon in their title bar. Under **Interval,** specify the number of seconds between refreshes.



Auto-refresh icon

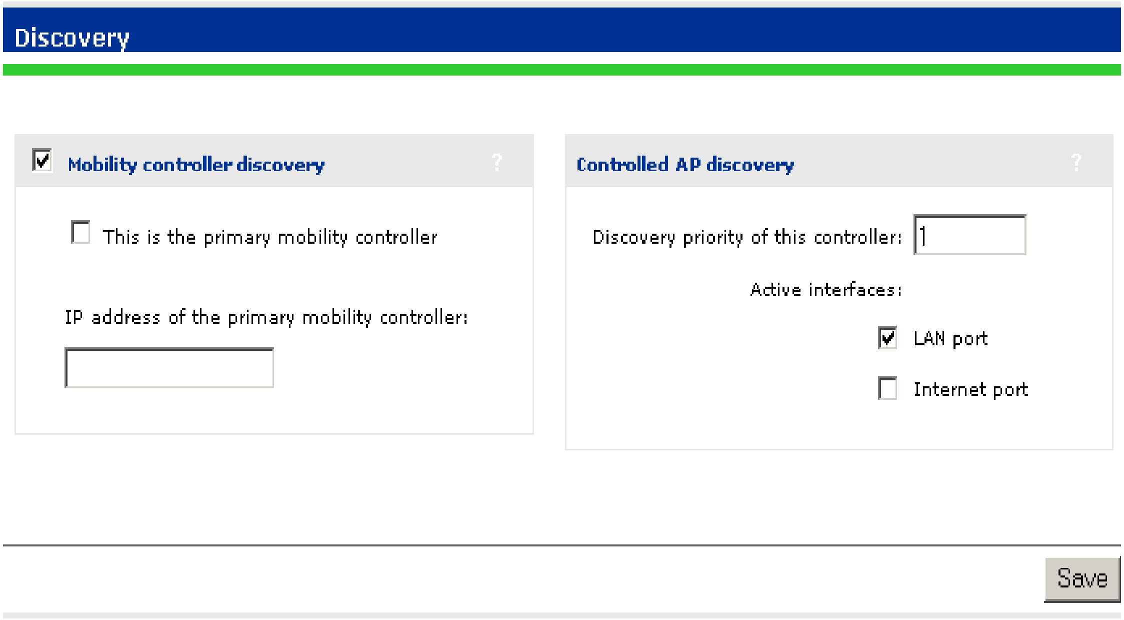
Figure 8-3: Auto-refresh

8.2 Device Discovery

Use this page to define discovery options for:

- inter-service controller discovery when using the mobility feature
- service controller discovery by controlled APs

Select **Management > Device discovery** to open the **Discovery configuration** page.



Discovery

☑ Mobility controller discovery

□ This is the primary mobility controller

IP address of the primary mobility controller:

Controlled AP discovery

Discovery priority of this controller: 1

Active interfaces:

☑ LAN port

□ Internet port

Figure 8-4: Device Discovery

8.2.1 Mobility Controller Discovery

Enable this option to either define this service controller as the primary mobility controller, or to have it connect to another service controller that is designated as the primary. For more information see "Wireless Mobility" on page 135.

8.2.1.1 The Primary Mobility Controller

Enable this option to designate this service controller as the primary mobility controller. The primary controller is responsible for the coordination and discovery of all service controllers in the mobile domain.

If you want service controllers to communicate with one another, then you must designate one service controller as the primary. On all other service controllers, disable this option and under **IP address of primary controller**, specify the IP address of the primary service controller.

By default, every service controller is configured to act as the primary mobility controller.

8.2.1.2 IP Address of Primary Mobility Controller

Enter the IP address of the primary mobility controller.

8.2.2 Controlled AP Discovery

8.2.2.1 Discovery Priority of this Controller

Sets the priority for this service controller when discovered by a controlled AP. A value of 1 indicates the highest priority. A value of 16 indicates the lowest priority.

If multiple service controllers are discovered by a controlled AP, the AP will establish a control channel with the service controller that has the highest priority setting first. If that service controller is already managing the maximum number of controlled APs, the AP will choose the service controller with the next highest priority.

8.2.2.2 Active Interfaces

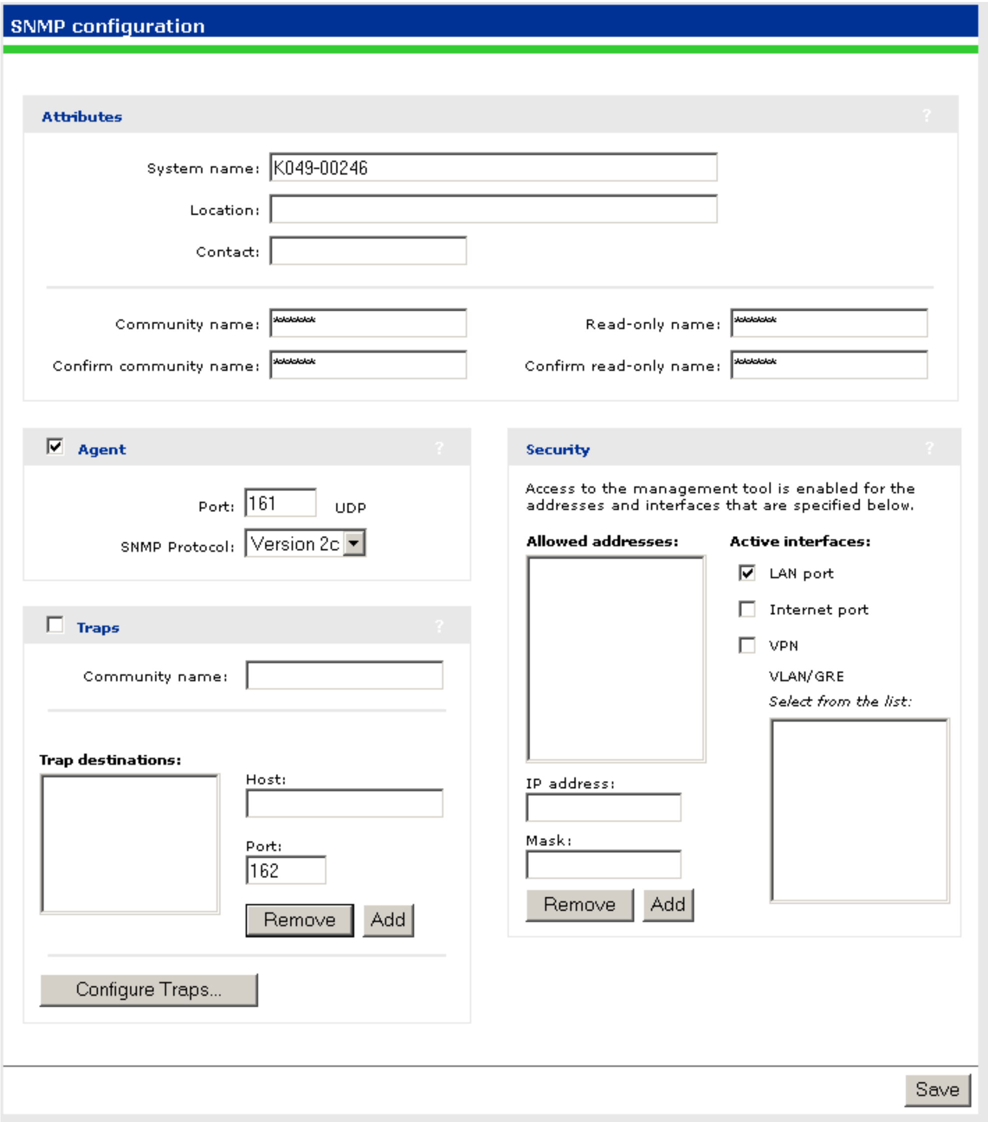
Select the physical interfaces on which the service controller will listen for discovery requests from controlled APs. The control channel to an AP is always established on the interface on which it is discovered.

8.3 SNMP

The service controller provides a robust SNMP implementation supporting both industry standard and Alvarion-specific MIBs. For complete information on supported MIBs, see the *SNMP MIB Reference Guide*.

8.3.1 Configuring SNMP Settings

Select **Management > SNMP** to open the **SNMP configuration** page. This page enables you to configure SNMP attributes, agents, traps, and security.



SNMP configuration

Attributes

System name: K049-00246

Location:

Contact:

Community name: ******

Read-only name: ******

Confirm community name: ******

Confirm read-only name: ******

☑ Agent

Port: 161 UDP

SNMP Protocol: Version 2c

☐ Traps

Community name:

Trap destinations:

Host:

Port: 162

Security

Access to the management tool is enabled for the addresses and interfaces that are specified below.

Allowed addresses:

IP address:

Mask:

Active interfaces:

☑ LAN port

☐ Internet port

☐ VPN

VLAN/GRE

Select from the list:

Figure 8-5: Configuring SNMP Settings

8.3.2 Attributes

- **System name**: Specify a name to identify the service controller. Default is the service controller’s serial number.
- **Location**: Specify a descriptive name for the location where the service controller is installed.
- **Contact**: Specify information about a contact person for the service controller.
- **Community name**: Specify the password that controls read/write access to SNMP information. A network management program must supply this password when attempting to **set** or **get** SNMP information from the service controller. By default, this is set to **private.**
- **Confirm community name**: Reenter the **Community name.**
- **Read-only name**: Specify the password that controls read-only access to the SNMP information. A network management program must supply this password when attempting to **get** SNMP information from the service controller. By default the **Read-only name** is **public.**
- **Confirm read-only name**: Reenter the **Read-only name.**

8.3.3 Agent

The SNMP agent is active by default. If you disable the agent the service controller will not respond to SNMP requests.

- **Port:** UDP port and protocol the service controller uses to respond to SNMP requests. Default port is 161.
- **SNMP Protocol:** SNMP version supported. Default is **Version 2c** which also supports requests from agents using version 1.

8.3.4 Security

Use these settings to control access to the SNMP interface.

- **Allowed addresses**: List of IP address from which access to the SNMP interface is permitted. To add an entry, specify the **IP address** and appropriate **Mask**, and then select **Add.**

- When the list is empty, access is permitted from any IP address.

- **Active interfaces**: Enable the checkboxes that correspond to the interfaces from which to allow access to the SNMP interface.

8.3.5 Traps

When this feature is enabled, the service controller sends traps to the hosts that appear in the **Traps destinations** list.

The service controller supports the following MIB II traps:

- coldStart
- linkUp
- linkDown
- authenticationFailure

In addition, the service controller supports a number of Alvarion-specific traps. Select **Configure Traps**. For a descriptions of these traps, see the online help.

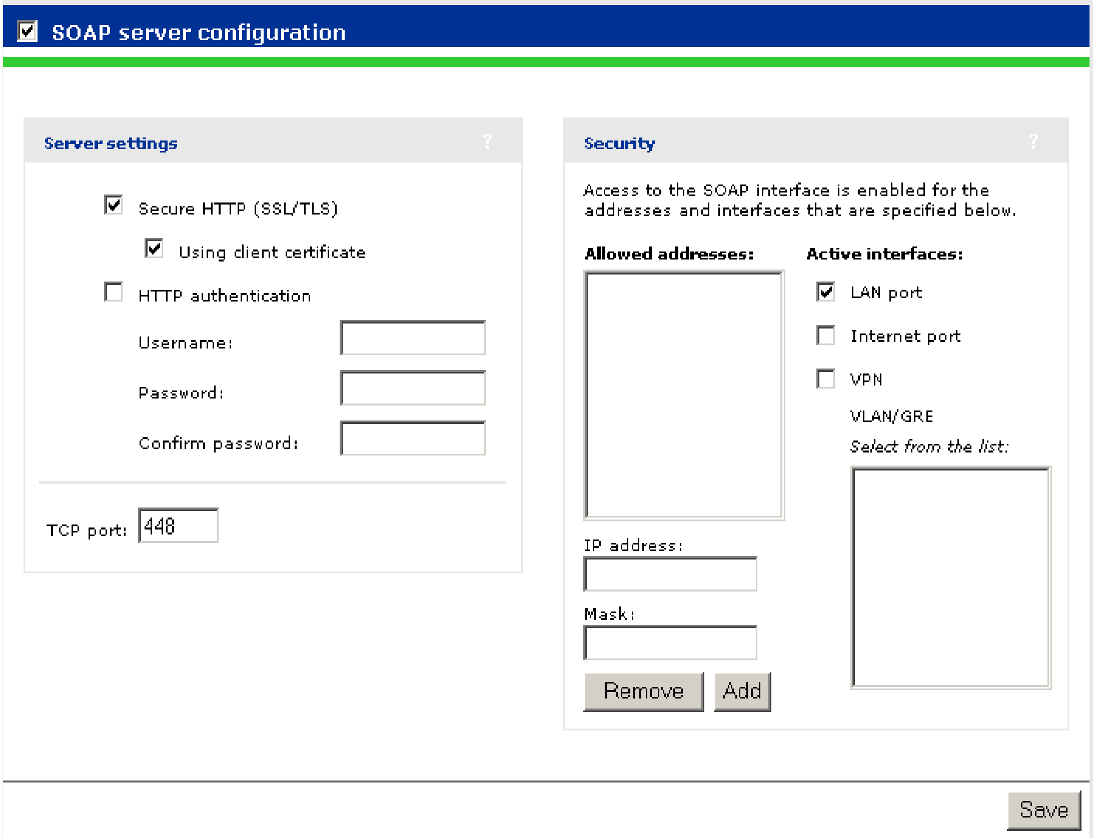
8.4 SOAP

The service controller provides a SOAP interface that can be used by SOAP-compliant client applications to perform configuration and management tasks.

For complete information using on the SOAP interface, see the insert SOAP package name here.

8.4.1 Configuring the SOAP Server

Select **Management > SOAP** to open the **SOAP server configuration** page. By default, the SOAP server is enabled.



☑ SOAP server configuration

Server settings

☑ Secure HTTP (SSL/TLS)

☑ Using client certificate

□ HTTP authentication

Username:

Password:

Confirm password:

TCP port: 448

Security

Access to the SOAP interface is enabled for the addresses and interfaces that are specified below.

Allowed addresses:

IP address:

Mask:

Active interfaces:

☑ LAN port

□ Internet port

□ VPN

VLAN/GRE

Select from the list:

Figure 8-6: Configuring the SOAP Server

8.4.1.1 Server Settings

8.4.1.1.1 Secure HTTP (SSL/TLS)

Enable this option to configure the SOAP server for SSL/TLS mode. When enabled, the Secure Sockets Layer (SSL) protocol must be used to access the SOAP interface.

8.4.1.1.2 Using Client Certificate

When enabled, the use of a X.509 client certificate is mandatory for SOAP clients.

8.4.1.1.3 HTTP Authentication

When enabled, access to the SOAP interface is available via HTTP with the specified username and password.

8.4.1.1.4 TCP Port

Specify the number of the TCP port that SOAP uses to communicate with remote applications. Default is 448.

8.4.1.1.5 Security

Use these settings to control access to the SOAP interface.

- **Allowed addresses**: List of IP address from which access to the SOAP interface is permitted. To add an entry, specify the **IP address** and appropriate **Mask**, and then select **Add.**

- When the list is empty, access is permitted from any IP address.

- **Active interfaces**: Enable the checkboxes that correspond to the interfaces from which to allow access to the SOAP interface.

8.4.1.2 Security Considerations

- The SOAP server is configured for SSL/TLS mode, and the use of a X.509 client certificate is mandatory for SOAP clients.

- The SOAP server is configured to trust all client certificates signed by the default Alvarion SOAP CA installed on the service controller.

- Users should generate and install their own SOAP CA private key/public key certificate to protect their devices from unauthorized access. This is important because the default SOAP CA and a valid client certificate are provided as an example to all customers. (See “Managing Certificates” on page 248.)

8.5 CLI

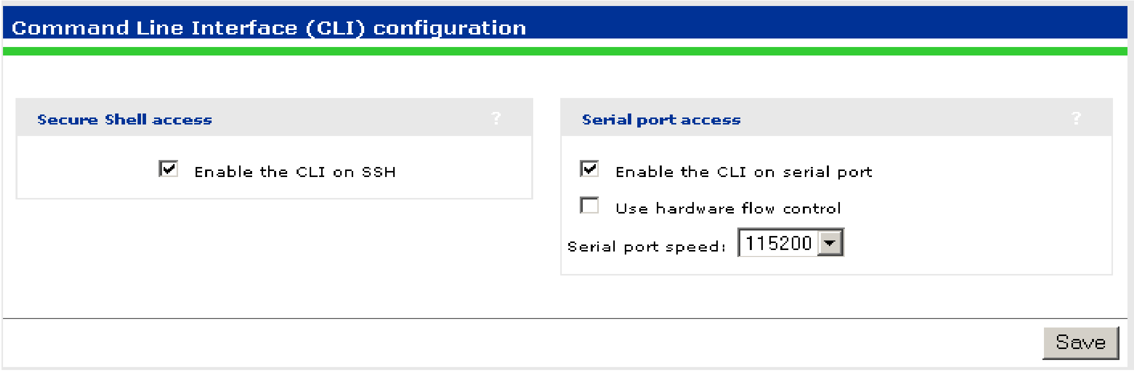
The service controller provides a command line interface that can be used to perform configuration and management tasks via the serial port or an IP connection on any of the service controller’s interfaces, including the LAN port, Internet port, or VPN/GRE tunnel.

For information on using the CLI, see the *Controller CLI Reference Guide*.

A maximum of three concurrent CLI sessions are supported regardless of the connection type.

8.5.1 Configuring CLI Support

Select **Management > CLI** to open the **Command Line Interface (CLI) configuration** page.



Command Line Interface (CLI) configuration

Secure Shell access

☑ Enable the CLI on SSH

Serial port access

☑ Enable the CLI on serial port

□ Use hardware flow control

Serial port speed: 115200

Figure 8-7: Configuring CLI Support

8.5.1.1 Secure Shell Access

Enable this option to allow access to the CLI via an SSH session. The CLI supports SSH on the standard TCP port (22).

Connectivity and login credentials for SSH connections use the same settings as defined for management tool administrators on the **Service controller >> Management > Management tool** page

- SSH connections to the CLI can be made on any active interface. Support for each interface must be explicitly enabled under **Security.**

- The login credentials for SSH connections are the same as those defined under **Administrator authentication**.

NOTE

SSH logins always use the local administrator username and password, even if **Administrator authentication** is set to use an external RADIUS server.

The following SSH clients have been tested with the CLI. Others may work as well:

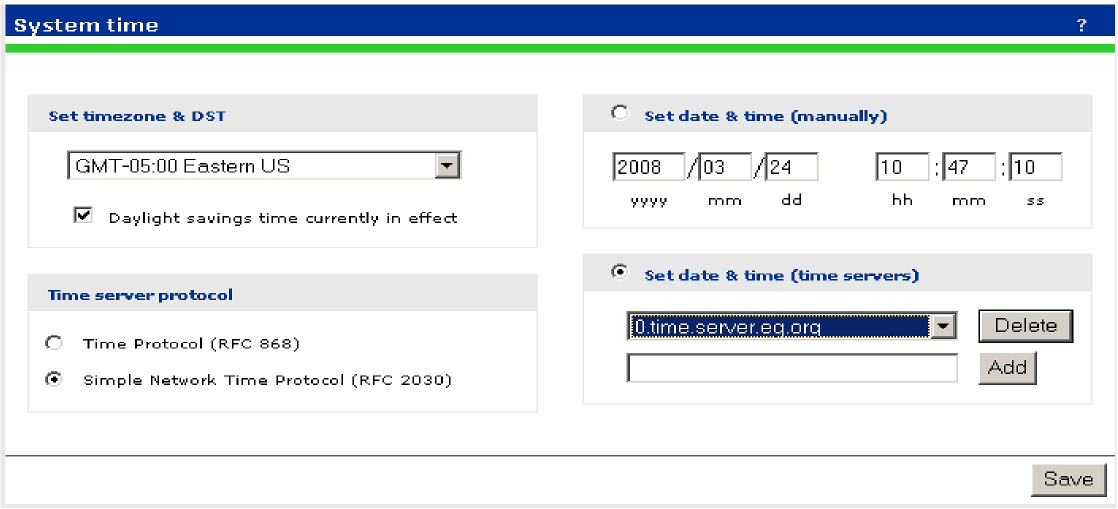
- OpenSSH
- Tectia
- SecureCRT
- Putty

8.5.1.2 Serial Port Access

- **Enable the CLI on serial port**: Enable this option to allow access to the CLI through the serial port.
- **Use hardware flow control**: Enable hardware flow control on the serial port connection. Flow control keeps the data flow at an efficient pace. Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be retransmitted.
- **Serial port speed**: Select the speed of your serial port connection.

8.6 System Time

Select **Management > System time** to open the **System time** page. This page enables you to configure the time server and time zone information.



System time ?

Set timezone & DST

GMT-05:00 Eastern US

☑ Daylight savings time currently in effect

Time server protocol

○ Time Protocol (RFC 868)

● Simple Network Time Protocol (RFC 2030)

○ **Set date & time (manually)**

2008 / 03 / 24 10 : 47 : 10

yyyy mm dd hh mm ss

● **Set date & time (time servers)**

0.time.server.eg.org

Figure 8-8: System Time

NOTE

Correct time is particularly important when the service controller is managing controlled APs, as the time configured on the service controller is used on all controlled APs. Synchronization and certificate problems can occur if the service controller time is not accurate.

1. Set **timezone & DST** as appropriate.
2. Set **Time server protocol** to **Simple Network Time Protocol** (default setting).
3. Select **Set date & time (time servers)** and then select the desired time server. TIme servers can be located on the Internet or LAN ports. **Add** other servers if desired. The service controller contacts the first server in the list. If the server does not reply, the service controller tries the next server and so on.
   The default setting is **ntp.org service**. This will resolve to a different registered time server each hour. For more information refer to:
   http://www.pool.ntp.org/
4. Select **Save** and verify that the date and time is updated accurately.

8.7 Country

NOTE

The Country sub-menu is not available on service controllers delivered with a fixed country setting. The country for which the service controller is configured to operate is displayed on the management tool home page.

Select **Management** > **Country** time to open the **Country** page. This page enables you to configure the country in which the service controller operates.

CAUTION

Do not change Country to a country other than the one in which the service controller operates. Failing to heed this caution may violate the regulatory compliance of controlled-mode APs managed by this service controller.

NOTE

After changing the country code controlled APs must be synchronized as described in "Synchronizing APs" on page 65.

9

Chapter 9 - Security

In This Chapter:

9.1 Using the Integrated RADIUS Server

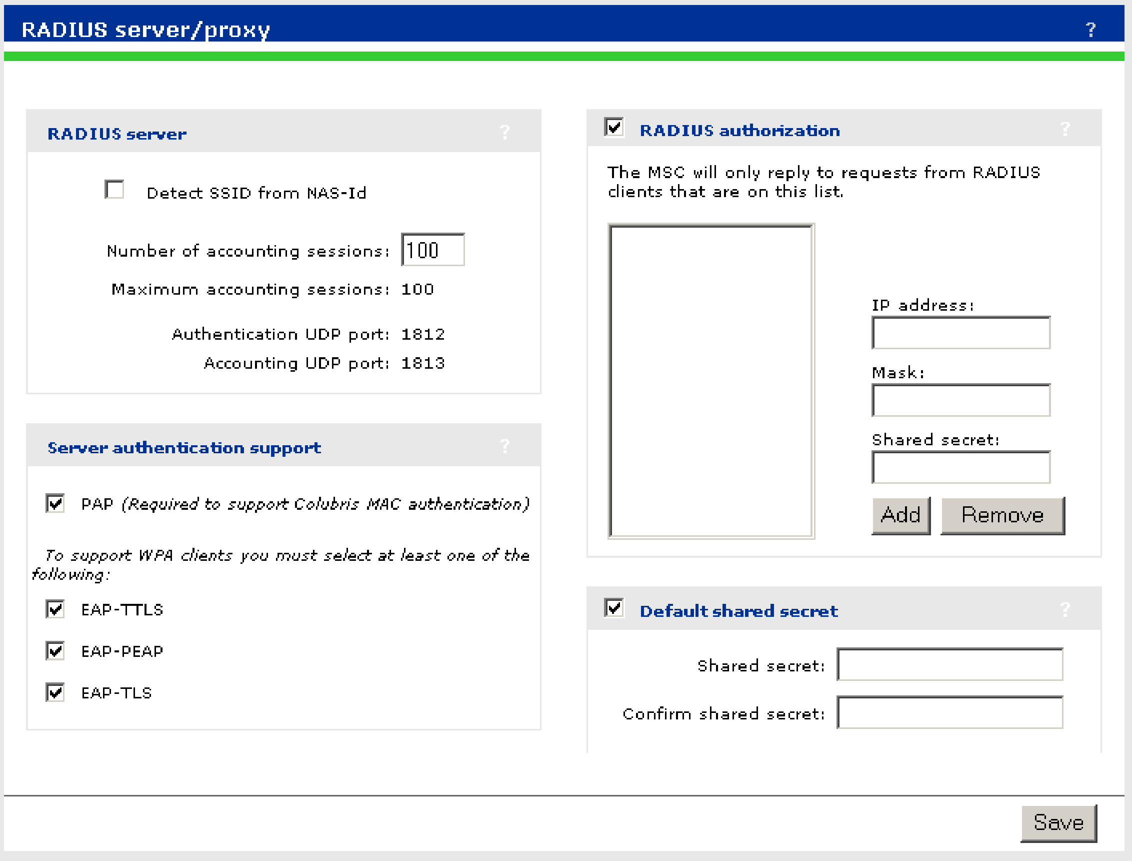
The internal RADIUS server is not intended as a replacement for the high-end/high-performance RADIUS server required for large scale deployments. Rather, it is offered as a cost-effective solution for user management for small hotspots or enterprise networks.

9.1.1 Primary Features

- Provides termination of 802.1X sessions at the service controller for clients using WPA/WPA2 with EAP-PEAP, EAP-TLS and EAP-TTLS. Support for other EAP protocols is viable using proxy mode.
- Provides MAC-based authentication of wireless users connected to both controlled and autonomous APs.
- Can be used to validate login credentials for HTML-based users.
- All locally defined user account options (user accounts, account profiles, and subscription plans) presented on the **Service Controller** >> **Users** menu are handled by the internal RADIUS server.
- Allows RADIUS accounting data to be sent to an external RADIUS server. (The internal RADIUS server does not provide support for accounting.)
- Local user accounts and account profiles have been designed to match the same functionality and support as can be provided by an external RADIUS server. Most of the AVPairs supported on an external RADIUS server are also supported by the integrated RADIUS server.

9.1.2 Server Configuration

Configuration of the integrated RADIUS server is done using the **Service Controller** >> **Security** > **RADIUS server** page. In most cases, the default settings on this page will not need to be changed.



RADIUS server/proxy

RADIUS server

□ Detect SSID from NAS-Id

Number of accounting sessions: 100

Maximum accounting sessions: 100

Authentication UDP port: 1812

Accounting UDP port: 1813

Server authentication support

☑ PAP *(Required to support Colubris MAC authentication)*

To support WPA clients you must select at least one of the following:

☑ EAP-TTLS

☑ EAP-PEAP

☑ EAP-TLS

☑ RADIUS authorization

The MSC will only reply to requests from RADIUS clients that are on this list.

IP address:

Mask:

Shared secret:

☑ Default shared secret

Shared secret:

Confirm shared secret:

Figure 9-1: Server Configuration

9.1.2.1 Configuration Parameters

9.1.2.1.1 RADIUS Server

9.1.2.1.1.1 Detect SSID from NAS-ID

Enable this option when working with autonomous third-party APs to permit the service controller to retrieve the SSID assigned to the AP, and therefore assign user traffic to the appropriate virtual network. For this to work, the AP must be configured to send its SSID as the NAS ID in all authentication and accounting requests. For more information, see "Working with Third-party Autonomous APs" on page 332.

9.1.2.1.1.2 Number of Accounting Sessions

Specify the maximum number of sessions for which the service controller will record accounting information.

9.1.2.1.1.3 Maximum Accounting Sessions

Specify the maximum number of accounting sessions that the service controller supports.

9.1.2.1.1.4 Authentication UDP Port

Indicates the port the service controller uses for authentication. This port is always set to the standard value of 1812.

9.1.2.1.1.5 Accounting UDP Port

Indicates the port the service controller uses for accounting. This port is always set to the standard value of 1813.

9.1.2.1.2 Server Authentication Support

Select the authentication protocols that the internal RADIUS server will support:

- PAP: This protocol must be enabled if any virtual networks are configured to use MAC-based authentication or HTML authentication.
- EAP-TTLS
- EAP-PEAP
- EAP-TLS

9.1.2.1.3 RADIUS Authorization

Applies to autonomous APs only. Requests from controlled APs are always accepted because they use the management tunnel.

Enable this option to restrict access to the RADIUS server. The RADIUS server will only respond to requests from RADIUS clients that appear in the list, or that match the default shared secret (below).

9.1.2.1.3.1 IP Address

Specify the IP address of the RADIUS client.

9.1.2.1.3.2 Mask

Specify the network mask.

9.1.2.1.3.3 Shared Secret

Specify the secret (password) that RADIUS client must use to communicate with the RADIUS server.

9.1.2.1.4 Default Shared Secret

Applies to autonomous APs only. Requests from controlled APs are always accepted because they use the management tunnel.

Enable this option to set a shared secret to safeguard communications between the internal RADIUS server and clients not in the RADIUS authorization list.

9.1.2.1.4.1 Shared Secret/confirm Shared Secret

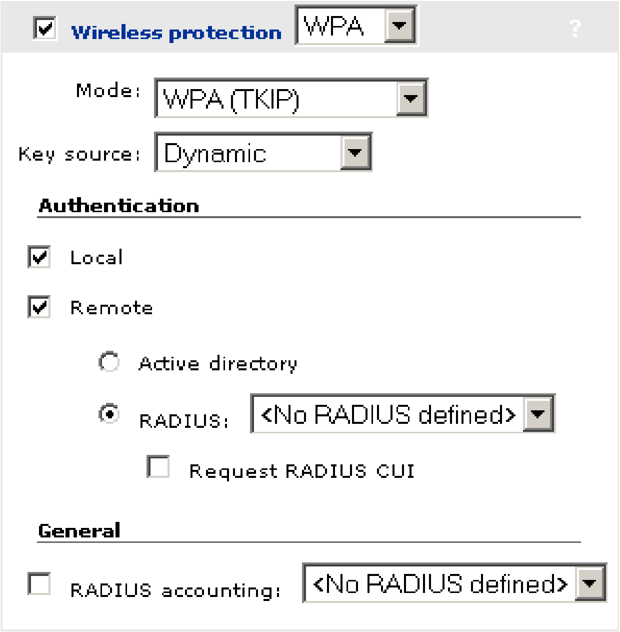
Specify the secret (password) that service controller will use when communicating with RADIUS clients that do not appear in the RADIUS authorization list. The shared secret must match on both the clients and the service controller.

9.1.3 User Account Configuration

User accounts for the internal RADIUS server are defined using the **Service Controller** >> **Users** menu. See “User Authentication” on page 259.

9.1.4 Assigning the Server to Virtual Network Authentication Tasks

To assign the integrated RADIUS server for authentication tasks in a virtual network, select the local option when configuring a virtual network profile. For example:



☑ Wireless protection: WPA

Mode: WPA (TKIP)

Key source: Dynamic

Authentication

☑ Local

☑ Remote

○ Active directory

● RADIUS: <No RADIUS defined>

□ Request RADIUS CUI

General

□ RADIUS accounting: <No RADIUS defined>

Figure 9-2: Assigning the Server for Authentication Tasks in a Virtual Network

9.2 Using a Third-party RADIUS Server

The service controller can use one or more RADIUS servers to perform a number of authentication and configuration tasks, including the tasks shown in the table below.

Task	For more information see
Validating administrator credentials	"Authenticating Administrators Using a RADIUS Server" on page 196
Validating user credentials for 802.1X, MAC, and HTML authentication types	"Wireless Protection" on page 111 "HTML-based User Logins" on page 114 "MAC-based Authentication" on page 115
Storing custom configuration settings for the public access interface	*Network Access Admin Guide*
Storing custom configuration settings for each user	
Storing accounting information for each user	

9.2.1 Configuring a RADIUS Client Profile on the Service Controller

The service controller enables you to define a maximum of 16 RADIUS profiles. Each profile defines the settings for a RADIUS client connection. To support a client connection, you must create a client account on the RADIUS server. The settings for this account must match the profile settings you define on the service controller.

For backup redundancy, each profile supports a primary and secondary server.

The service controller can function with any RADIUS server that supports RFC 2865 and RFC 2866. Authentication occurs via authentication types such as: EAP-MD5, CHAP, MSCHAP v1/v2, PAP, EAP-TLS, EAP-TTLS, EAP-PEAP. EAP-SIM, EAP-AKA, EAP-FAST, and EAP-GTC.

CAUTION

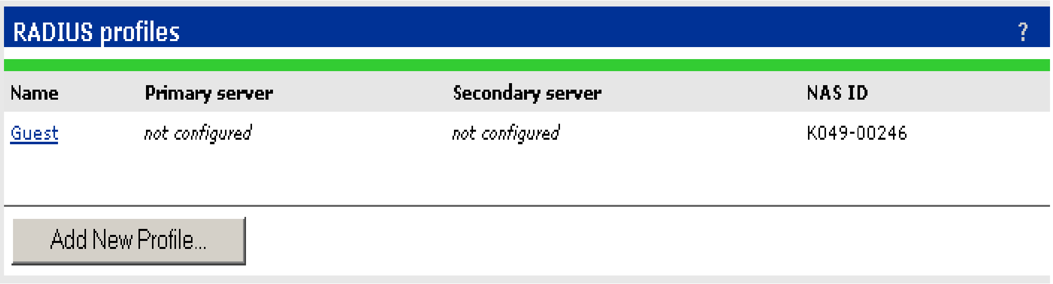
To safeguard the integrity of the RADIUS traffic, it is important that you protect communications between the service controller **and the RADIUS server. The** service controller **lets you use PPTP or IPSec to create a secure tunnel to the RADIUS server. For complete instructions on how to accomplish this, see** "Creating VPN Connections" on page 236

NOTE

If you change a RADIUS profile to connect to a different server while users are active, all RADIUS traffic for active user sessions is immediately sent to the new server.

9.2.1.1 Configuration Procedure

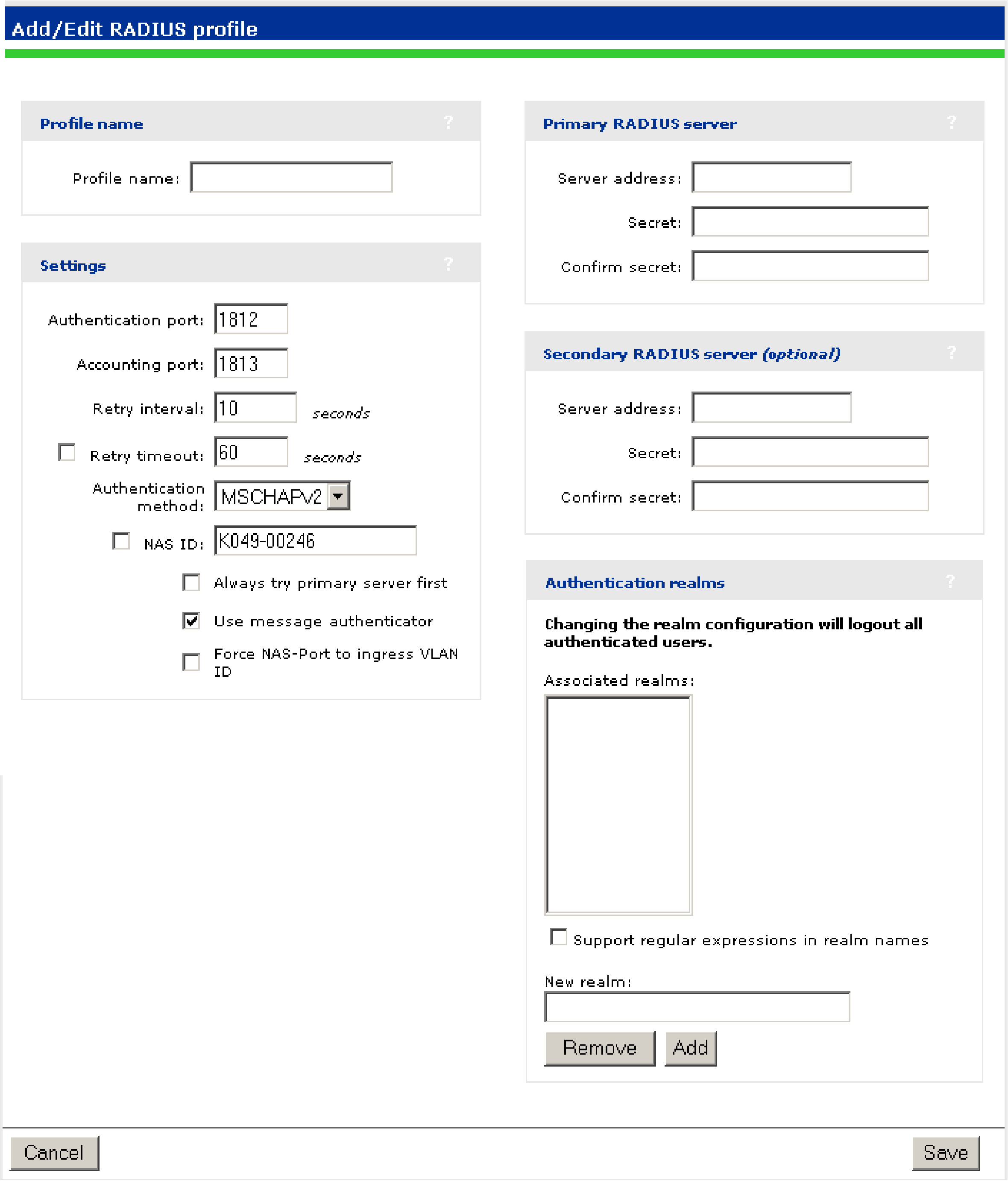
1 Select **Service Controller** >> **Security** > **RADIUS profiles.** The RADIUS profiles page opens.



Name	Primary server	Secondary server	NAS ID
Guest	*not configured*	*not configured*	K049-00246

Figure 9-3: Radius Profiles

2 Select **Add New Profile.** The Add/Edit RADIUS Profile page opens.



Add/Edit RADIUS profile

Profile name

Profile name:

Settings

Authentication port: 1812

Accounting port: 1813

Retry interval: 10 *seconds*

□ Retry timeout: 60 *seconds*

Authentication method: MSCHAPv2

□ NAS ID: K049-00246

□ Always try primary server first

☑ Use message authenticator

□ Force NAS-Port to ingress VLAN ID

Primary RADIUS server

Server address:

Secret:

Confirm secret:

Secondary RADIUS server *(optional)*

Server address:

Secret:

Confirm secret:

Authentication realms

Changing the realm configuration will logout all authenticated users.

Associated realms:

□ Support regular expressions in realm names

New realm:

Figure 9-4: Adding a Radius Profile

3 Configure the profile settings as described in the following Configuration Parameters section.

4 Select **Save**.

9.2.1.2 Configuration Parameters

9.2.1.2.1 Profile Name

Specify a name to identify the profile.

9.2.1.2.2 Settings

- **Authentication port:** Specify a port on the RADIUS server to use for authentication. By default RADIUS servers use port 1812.
- **Accounting port:** Specify a port on the RADIUS server to use for accounting. By default RADIUS servers use port 1813.
- **Retry interval:** Specify the number of seconds that the RADIUS server waits before access and accounting requests time out. If the server does not receive a reply within this interval, the service controller switches between the primary and secondary RADIUS servers, if a secondary server is defined. A reply that is received after the retry interval expires is ignored.

  Retry interval applies to access and accounting requests that are generated by the following:

  - Administrator access to the management tool
  - User authentication by way of HTML
  - MAC-based authentication of devices
  - Authentication of the service controller
  - Authentication of the controlled AP

  You can determine the maximum number of retries as follows:

  - HTML-based logins: Calculate the number of retries by taking the setting for the HTML-based logins **Authentication Timeout** parameter and dividing it by the value of this parameter. Default settings result in 4 retries (40 / 10).
  - MAC-based and service controller authentication: Number of retries is infinite.
  - 802.1X authentication: Retries are controlled by the 802.1X client software.

- **Authentication method:** Select the default authentication method that the service controller uses when exchanging authentication packets with the RADIUS server defined for this profile.
- For 802.1X users, the authentication method is always determined by the 802.1X client software and is not controlled by this setting.
- If traffic between the service controller and the RADIUS server is not protected by a VPN, it is recommended that you use either EAP-MD5 or MSCHAP V2 (if supported by your RADIUS Server). PAP, and MSCHAP V1 are less secure protocols.
- **NAS ID:** Specify the identifier for the network access server that you want to use for the service controller. By default the serial number of the service controller is used. The service controller includes the NAS-ID attribute in all packets that it sends to the RADIUS server.
- **Always try primary server first:** Enable this option if you want to force the service controller to contact the primary server first.

  Otherwise, the service controller sends the first RADIUS access request to the last known RADIUS server that replied to any previous RADIUS access request. If the request times out, the next request is sent to the other RADIUS server if defined.

  For example, assume that the primary RADIUS server was not reachable and that the secondary server responded to the last RADIUS access request. When a new authentication request is received, the service controller sends the first RADIUS access request to the secondary RADIUS server.

  If the secondary RADIUS server does not reply, the service controller retransmits the RADIUS access request to the primary RADIUS server. When two servers are configures, the service controller always alternates between the two.

9.2.1.2.3 Primary/Secondary RADIUS Server

- **Server address:** Specify the IP address of the RADIUS server.
- **Secret/Confirm secret:** Specify the password for the service controller to use to communicate with the RADIUS server. The shared secret is used to authenticate all packets exchanged with the server, proving that the packets originate from a valid/trusted source.

9.2.1.2.4 Authentication Realms

When authentication realms are enabled for a profile, selection of the RADIUS server to use for authentication is based on the realm name, rather than the RADIUS profile name configured. This applies to any virtual network authentication setting that uses the profile.

- Realm names are extracted from user names as follows: if the username is **person1@mydomain.com** then **mydomain.com** is the realm. The authentication request is sent to the RADIUS profile with the realm name **mydomain.com**. The username sent for authentication is still the complete **person1@mydomain.com**.
- For added flexibility, regular expressions can be used in realm names, enabling a single realm name to match many users. For example, if a realm name is defined with the regular expression **`^per.*`** then all usernames beginning with **per** followed by any number of characters will match. The following usernames would all match:

  per123.biz
  per321.lan
  per1

9.2.1.2.5 Important

- You must enable the use of authentication realms for the virtual network.
- Realms names are not case-sensitive and can be a maximum of 64 characters long.
- You can define a maximum of 200 realms across all RADIUS profiles. There is no limit to the number of realms that you can define for each RADIUS profile.
- Each RADIUS profile can be associated with one or more realms. However, a realm cannot be associated with more than one profile.
- A realm overrides the authentication RADIUS server only; the server used for accounting is not affected.

⚠ **CAUTION**

When realm configuration is changed in any way, all active user sessions are terminated.

9.3 Using an Active Directory Server

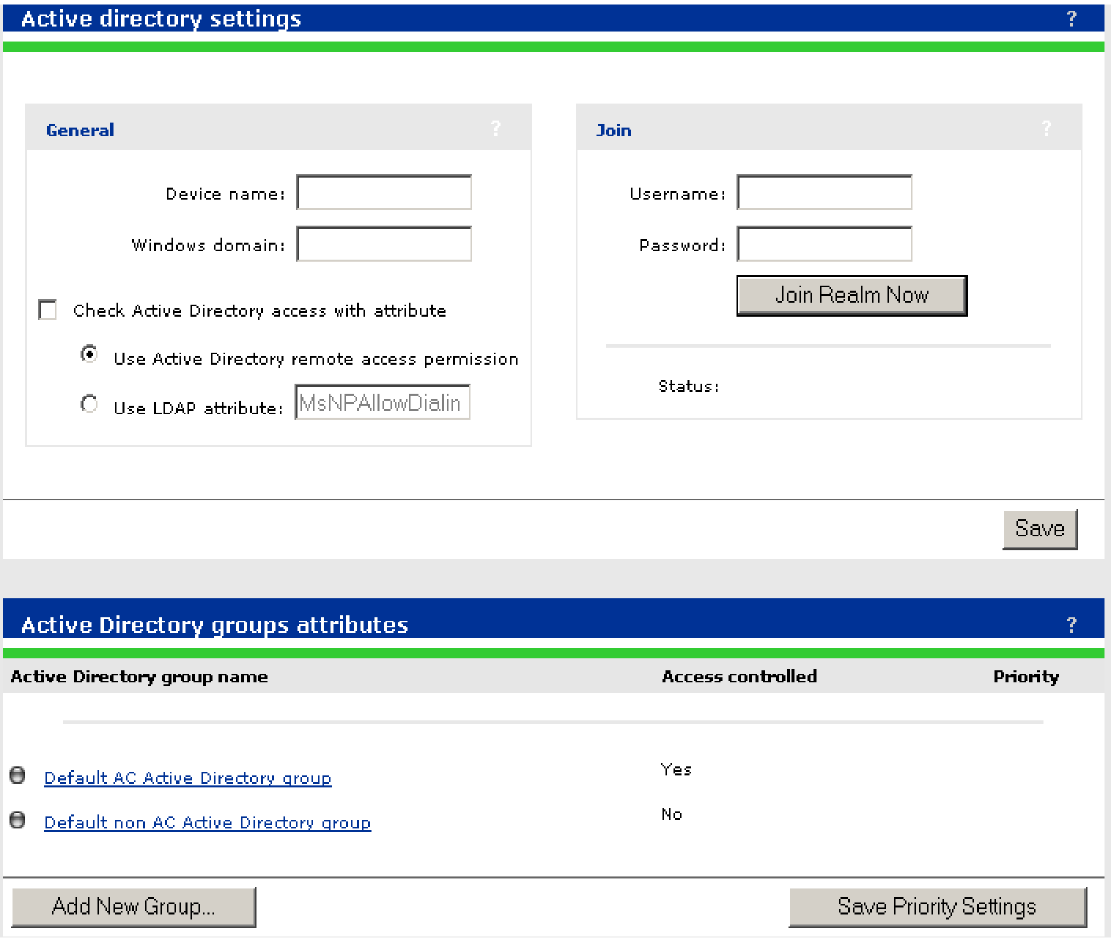
The service controller can be configured to validate user login credentials using an *external* Active Directory server for the following virtual network features:

- Wireless Protection (only WPA and WPA2 both with EAP-PEAP)
- HTML-based logins

Once a user is authenticated by Active Directory, the service controller retrieves the names of all the active directory groups of which the user is a member and uses them to activate appropriate configuration settings for the user locally-defined on the service controller.

9.3.1 Active Directory Configuration

To configure active directory support, select **Service Controller** >> **Security** > **Active Directory**.



Active directory settings ?

General ?

Device name:

Windows domain:

□ Check Active Directory access with attribute

● Use Active Directory remote access permission

○ Use LDAP attribute: MsNPAllowDialin

Join ?

Username:

Password:

Join Realm Now

Status:

Save

Active Directory groups attributes ?

Active Directory group name	Access controlled	Priority
Default AC Active Directory group	Yes	
Default non AC Active Directory group	No	

Add New Group...

Save Priority Settings

Figure 9-5: Active Directory Configuration

9.3.1.1 Active Directory Settings

9.3.1.1.1 General

9.3.1.1.1.1 Device Name

Specify a name that identifies the service controller to Active Directory. The service controller uses this name to connect to the active directory server, just like any standard active directory client does.

9.3.1.1.1.2 Windows Domain

Specify the Windows domain to which the service controller belongs. The service controller must be part of a Windows domain (**mydomain.com**, for example) to authenticate users that belong to that domain.

9.3.1.1.1.3 Check Active Directory Access with Attribute

Enable this option to have the service controller only accept users with a specific setting in their account.

- **Use Active Directory remote access permission:** Use the standard attribute defined in Active Directory for remote access (MsNPAllowDIalin). If this attribute is set, then the user can be authenticated via Active Directory.
- **Use LDAP attribute:** For non-standard implementation of Active Directory, set this according to the equivalent setting on the Active Directory server.

9.3.1.1.2 Join

Before the service controller can process user authentication using Active Directory, you must join the service controller with the Active Directory server. Fill in the required parameters and click **Join Realm Now**. This is usually a one-time event.

9.3.1.1.2.1 Username

Username the service controller will use to join Active Directory.

9.3.1.1.2.2 Password

Password the service controller will use to join Active Directory.

NOTE

For security reasons, **Username** and **Password** are not stored on the service controller.

9.3.1.1.2.3 Join Realm Now

Select to join the realm immediately.

9.3.1.1.2.4 Status

Shows the status of the join operation as follows:

- **Unknown:** System is processing, no status to report. Refresh the page to update the status.
- **DNS unavailable:** DNS not working, cannot access Active Directory.
- **Missing Config:** No configuration, so join cannot proceed.
- **Never Joined:** Administrator never selected **Join Realm Now**.
- **Not joined:** Not joined: May have be joined with the domain, but the join was not confirmed yet. Status will changed to **Joined** once confirmed. Check connectivity between the service controller and Active Directory or re-join.
- **Joined:** Active Directory reports that service controller successfully joined.

9.3.1.2 Active Directory Group Attributes

Displays all Active Directory groups that are defined on the service controller. These groups are used to assign attributes to a user once they have been authenticated by Active Directory.

NOTE

Group names on the service controller must be identical to existing Active Directory Organizational Units configured on the Active Directory Server.

Once a user is authenticated by Active Directory, the service controller retrieves the names of all the active directory groups of which the user is a member.

- If the user is a member of only one Active Directory group, and that group name appears in the list, the service controller applies the attributes from that group.
- If the user is a member of more than one Active Directory group, the service controller applies the attributes from the matching group name with the highest priority (highest in the list).
- If no match is found, the attributes defined for one of the default groups are applied as follows:
  - If the virtual network the user logged in on is access-controlled then the **Default AC Active Directory** group is used.
  - If the virtual network the user logged in on is not access-controlled then the **Default non AC Active Directory** group is used.

NOTE

The default groups are disabled by default. You need to enable them before they can be used.

9.3.1.2.1 Add New Group

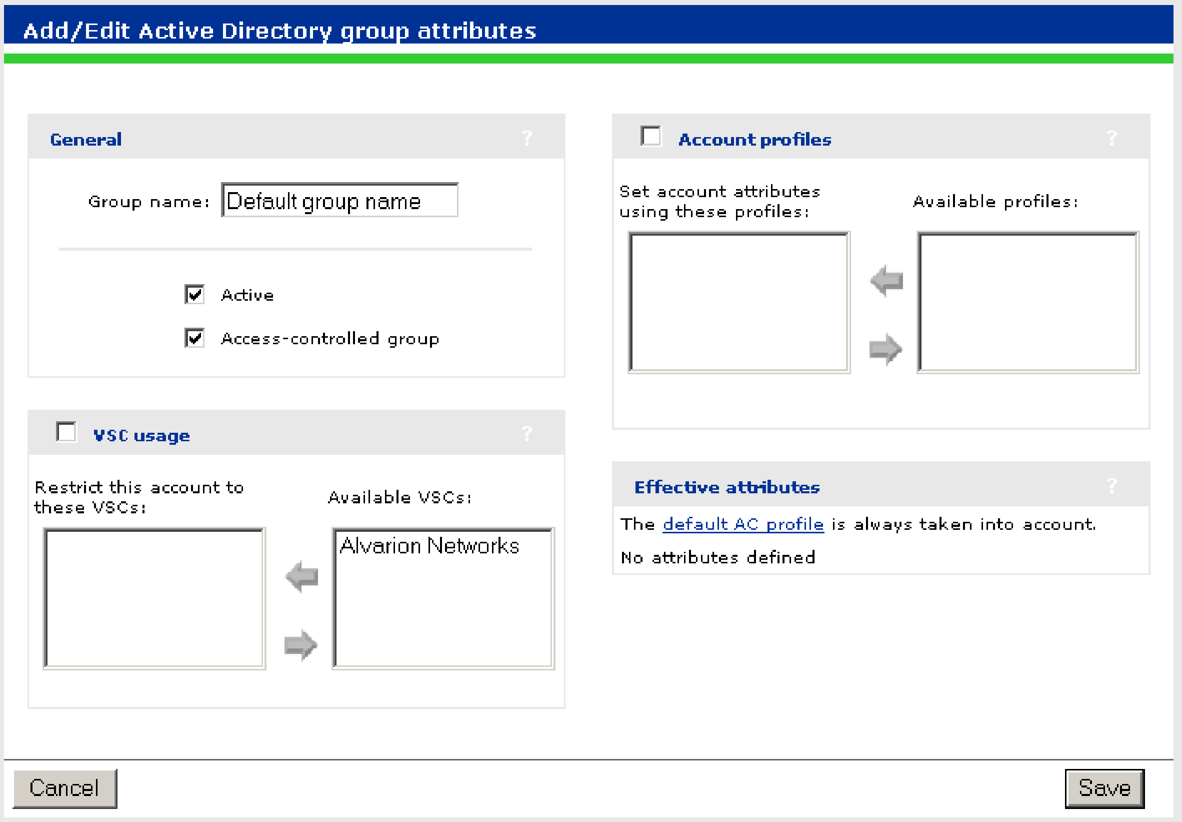
Select to add a new group. See “Configuring an Active Directory Group” on page 226 for configuration details.

9.3.1.2.2 Save Priority Settings

After using the up/down arrows to change the priority of groups, save your changes by selecting this button.

9.3.2 Configuring an Active Directory Group

An active directory group defines the characteristics of a user session. To make group configuration easy, account profiles ("Account Profiles" on page 267) can be applied to set group attributes.



Add/Edit Active Directory group attributes

General

Group name: Default group name

☑ Active

☑ Access-controlled group

□ VSC usage

Restrict this account to these VSCs:

Available VSCs: Alvarion Networks

□ Account profiles

Set account attributes using these profiles:

Available profiles:

Effective attributes

The default AC profile is always taken into account.

No attributes defined

Figure 9-6: Configuring an Active Directory Group

9.3.2.1 Configuration Parameters

9.3.2.1.1 General

9.3.2.1.1.1 Group Name

Specify a name to identify the group. This name must exactly match an existing Active Directory Organizational Unit configured on the Active Directory Server.

9.3.2.1.1.2 Active

Enable this option to activate the group. The group cannot be used until it is active.

9.3.2.1.1.3 Access-controlled Group

Determines whether the group is access-controlled or not.

- Access-controlled groups can only be used to login on virtual networks that are access-controlled.
- Non access-controlled groups can only be used to login on virtual networks that are not access-controlled.

9.3.2.1.2 Virtual Network Usage

Enable this option to restrict this group to one or more virtual networks. If the selected virtual networks are not defined on an AP, users will not be able to login on this account.

The **Available virtual networks** list shows all defined virtual networks that you can select from.

To move virtual networks between the two lists:

- Double-click the profile you want to move.
- Or, select the profile you want to move and then click the left or right arrow.

9.3.2.1.3 Account Profiles

Enable this option to set the attributes of this group using one or more account profiles.

The **Available profiles** list shows all defined profiles that you can select from. (To add a new profile, open the **Service Controller** >> **Users** > **Account profiles** page.)

To move profiles between the two lists, double-click the profile you want to move, or select the profile you want to move and then select the left or right arrow.

9.3.2.1.4 Effective Attributes

This list shows all attributes that are active for the group.

Each time you add an account profile for use by this group, all attributes in the profile are added to the list.

NOTE

Each profile that is applied to a group must have a unique set of attributes. The same attribute cannot be present in two different account profiles.

9.3.2.1.4.1 About the Default AC Profile

The **Default AC profile** is created by the service controller and is always applied to all groups. It provides access to the values of any user-applicable attributes that are defined on the **Service Controller >> Public access > Attributes** page, and includes attributes retrieved from a RADIUS server or configured attributes.

For example, the **Default AC profile** provides access to the value of the following attributes (if defined):

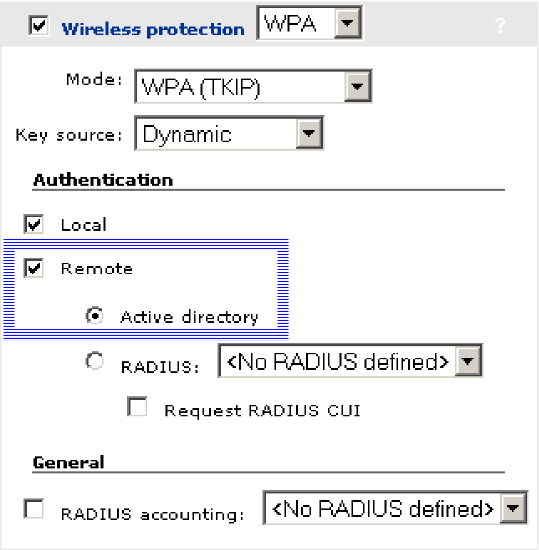
- DEFAULT-USER-ACCT-INTERIM-UPDATE
- DEFAULT-USER-MAX-INPUT-PACKETS
- DEFAULT-USER-MAX-OUTPUT-PACKETS
- DEFAULT-USER-MAX-TOTAL-PACKETS
- DEFAULT-USER-MAX-INPUT-OCTETS
- DEFAULT-USER-MAX-OUTPUT-OCTETS
- DEFAULT-USER-MAX-TOTAL-OCTETS
- DEFAULT-USER-IDLE-TIMEOUT
- DEFAULT-USER-SMTP-REDIRECT
- DEFAULT-USER-SESSION-TIMEOUT
- DEFAULT-USER-ONE-TO-ONE-NAT

9.4 Configuring a Virtual Network to Use Active Directory for Authentication Tasks

Any virtual network feature that can be configured to support remote authentication can be configured to use Active Directory. This includes:

- Wireless protection
- HTML-based user logins

For example:



☑ Wireless protection WPA

Mode: WPA (TKIP)

Key source: Dynamic

Authentication

☑ Local

☑ Remote

● Active directory

○ RADIUS: <No RADIUS defined>

□ Request RADIUS CUI

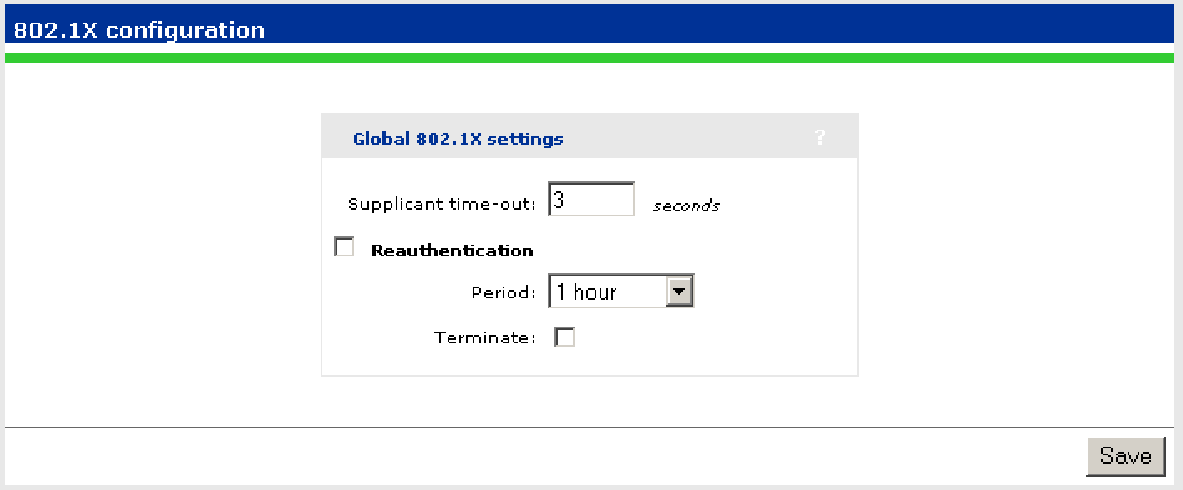
General

□ RADIUS accounting: <No RADIUS defined>

Figure 9-7: Wireless Protection: Configured to Use Active Directory

9.5 Configuring Global 802.1X Settings

The service controller provides several 802.1X settings that apply globally to all 802.1X connections. To configure these settings, select **Security > 802.1X**.



802.1X configuration

Global 802.1X settings

Supplicant time-out: 3 *seconds*

□ **Reauthentication**

Period: 1 hour

Terminate: □

Figure 9-8: 802.1X Configuration

Configurable parameters on the **802.1X configuration** page include the following:

- **Supplicant timeout:** Specify the maximum length of time the service controller will wait for a client station to respond to an EAPOL packet before resending it.
- If wireless client stations are configured to manually specify the 802.1X username or password, or both, increase the value of the timeout to between 15 and 20 seconds.
- **Reauthentication**: Enable this option to force 802.1X clients to reauthenticate after the specified **Period**. This option is disabled by default.
  - **Period**: Client stations must reauthenticate after this amount of time has passed since their last reauthentication.
  - **Terminate**: Specifies how client traffic is handled during reauthentication.
    - **Disabled**: Client stations remain connected during reauthentication and traffic is blocked only if reauthentication fails.

- **Enabled**: Client traffic is blocked during reauthentication and is activated again only if authentication succeeds.

9.6 Firewall

To safeguard your network from intruders, the service controller features a customizable stateful firewall. The firewall operates on the traffic streaming through the Internet port. It can be used to control both incoming and outgoing data.

The service controller features a number of predefined firewall rules to let you achieve the security level you need without going to the trouble of designing your own rules. You can create a completely custom set of firewall rules to suit your particular networking requirements, if necessary.

If the service controller is connected to a wired LAN, the firewall protects the wired LAN as well.

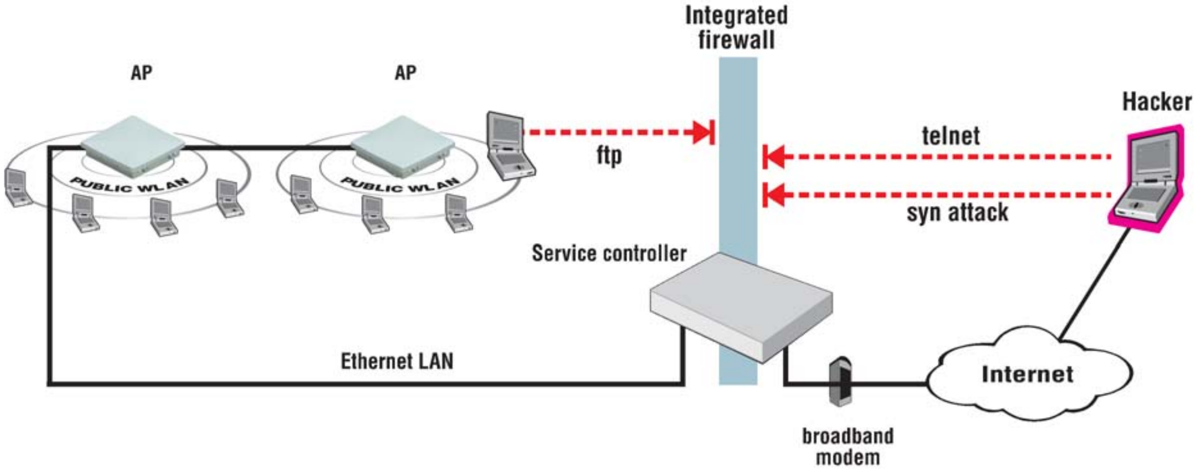


Figure 9-9: Firewall

9.6.1 Firewall Presets

The easiest way to use the firewall is to use one of the preset settings. Two levels of security are provided:

- **High**: Permits all outgoing traffic, except NetBIOS (TCP and UDP). Blocks all externally initiated connections.
- **Low**: Permits all incoming and outgoing traffic, except for NetBIOS traffic. Use this option if you require active FTP sessions.

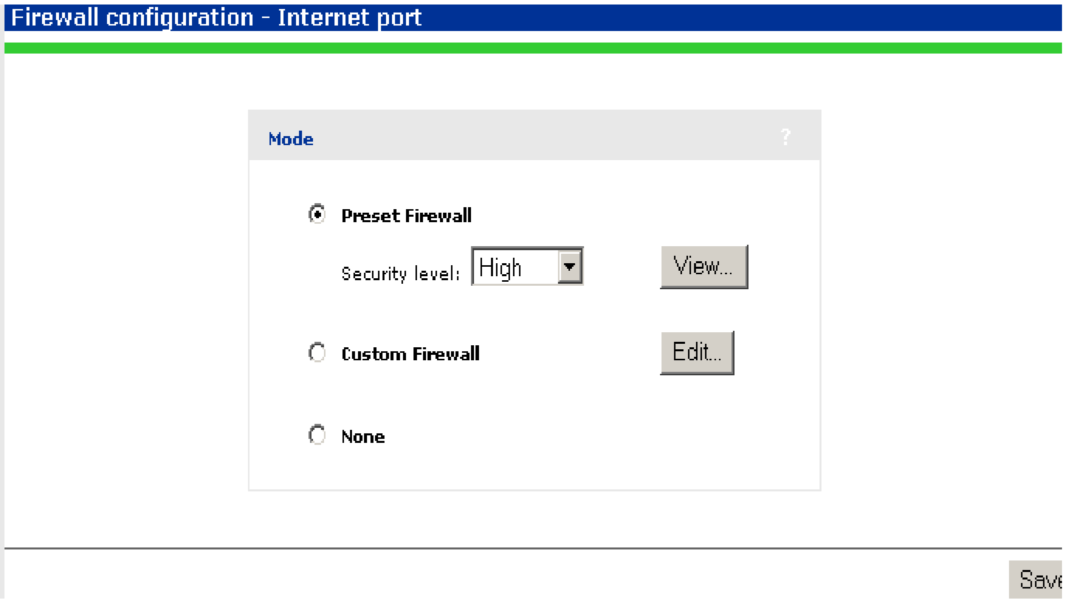
The following tables indicate how some common applications are affected by the preset firewall settings.

Outgoing traffic	Firewall setting	
Application	**Low**	**High**
FTP (passive mode)	Passed	
FTP (active mode)	Passed	
Web (HTTP, HTTPS)	Passed	
SNMP	Passed	
Telnet	Passed	
Windows networking	Blocked	
ping	Passed	
PPTP from client station to remote server	Passed	
NetMeeting (make call)	Passed	
IPSec pass-through	Passed	
NetBIOS	Blocked	

Incoming traffic	Firewall setting	
Application	**Low**	**High**
FTP (passive mode)	Passed	Blocked
FTP (active mode)	Passed	Blocked
Web (HTTPS)	Passed	Blocked
Web (HTTP)	Passed	Blocked
Telnet	Passed	Blocked
Windows networking	Passed	Blocked
PPTP from remote client to a server on the local network	Passed	Blocked
ping client on local network	Passed	Blocked
IPSec pass-through	Passed	Blocked
NetBIOS	Passed	Blocked
NetMeeting (receive call)	Passed	Blocked

9.6.2 Firewall Configuration

To configure a firewall, select **Security > Firewall**. The **Firewall configuration** page opens.



Firewall configuration - Internet port

Mode

● Preset Firewall

Security level: High

○ Custom Firewall

○ None

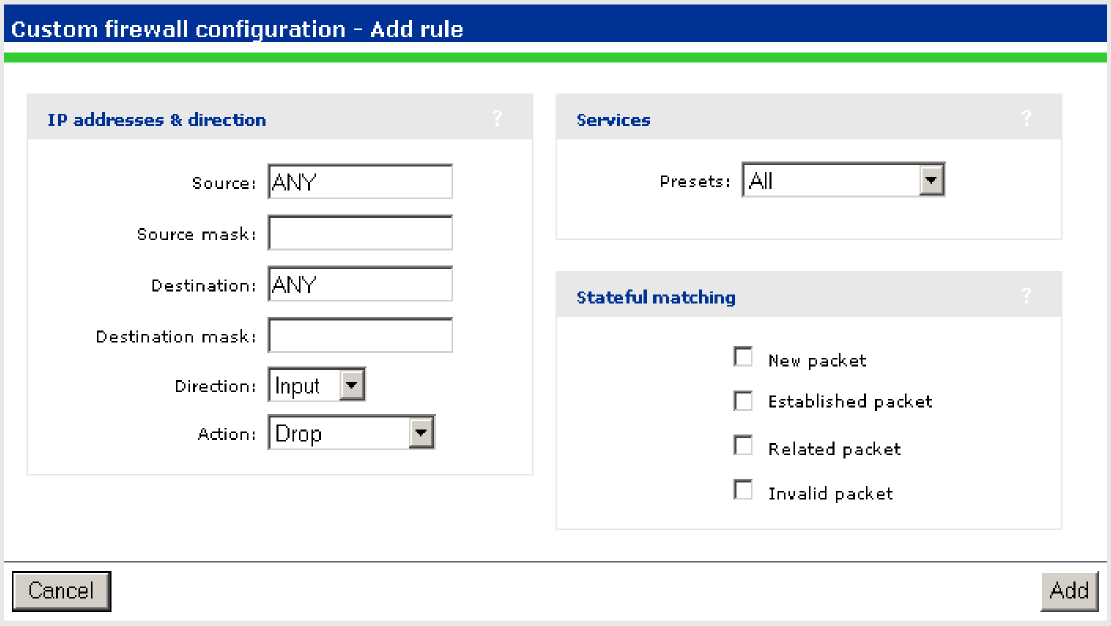
Figure 9-10: Firewall Configuration

- Select **Preset firewall** to use a preconfigured firewall setting of **High** or **Low.** Select **View** to see the firewall rules for the selected setting.
- Select **Custom firewall** if you have specific security requirements. This setting enables you to target specific protocols or ports.

9.6.3 Customizing the Firewall

To customize the firewall, you define one or more rules. A rule lets you target a specific type of data traffic. If the service controller finds data traffic that matches the rule, the rule is triggered, and the traffic is rejected or accepted by the firewall.

To add a rule, select **Custom Firewall** on page **Security > Firewall**, select **Edit**, and then select **Add New Rule**.



Custom firewall configuration - Add rule

IP addresses & direction

Source: ANY

Source mask:

Destination: ANY

Destination mask:

Direction: Input

Action: Drop

Services

Presets: All

Stateful matching

□ New packet

□ Established packet

□ Related packet

□ Invalid packet

Figure 9-11: Customizing the Firewall

Rules operate on IP datagrams (sometimes called *packets).* Datagrams are the individual packages of data that travel on an IP network. Each datagram contains addressing and control information along with the data it is transporting. The firewall analyses the addressing and control information to apply the rules you define.

The service controller applies the firewall rules in the order that they appear in the list. An intelligent mechanism automatically adds the new rules to the list based on their scope. Rules that target a large amount of data are added at the bottom. Rules that target specific datagram attributes are added at the top.

9.7 Creating VPN Connections

The service controller features virtual private network (VPN) software that enables it to create a secure connection to a remote site by way of a non-secure infrastructure like the Internet.

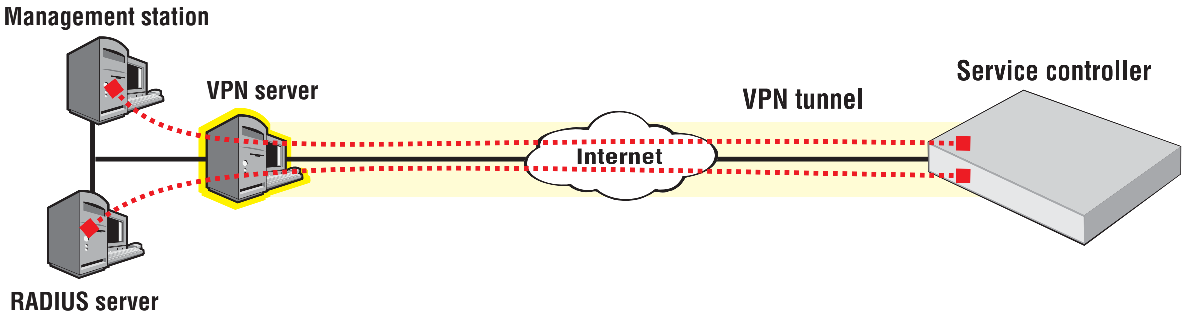


Figure 9-12: VPN Connections

Two options are available: PPTP client and IPSec.

- decode the packets of data being exchanged between two IPSec peers.

NOTE

Traffic in the VPN tunnel bypasses the service controller’s firewall.

CAUTION

The VPN tunnel should not be used to transport user traffic. The tunnel should only be used to carry management traffic. (RADIUS, SNMP, and management sessions).

To prevent user traffic from entering the tunnel, you must define access list definitions to DENY access to all subnets on the other side of the tunnel.

Consider the following scenario:

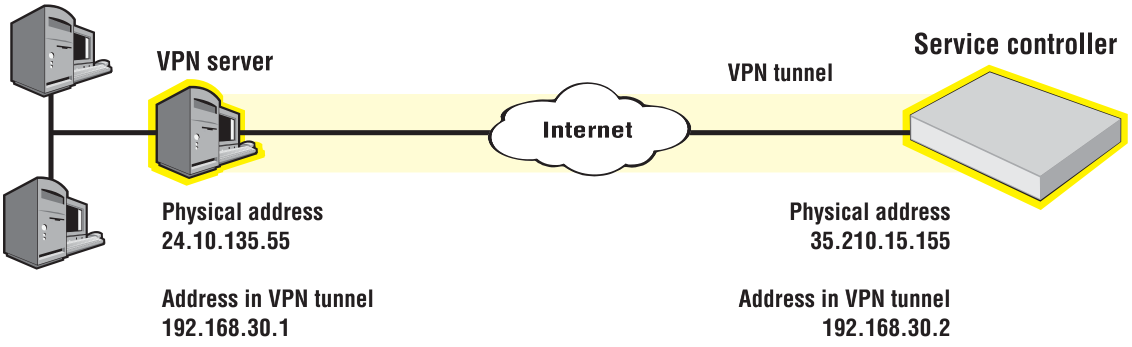


Figure 9-13: VPN Connection Scenario

To protect the VPN, add the following definitions to the site access list:

```
access-list=vpn,DENY,all,192.168.30.0/24,all
use-access-list=vpn
```

This definition applies to all users, whether they are authenticated or not. It blocks access to the VPN subnet for all traffic. For more information on using the access list feature, see the *Network Access Admin Guide*.

9.7.1 PPTP Client

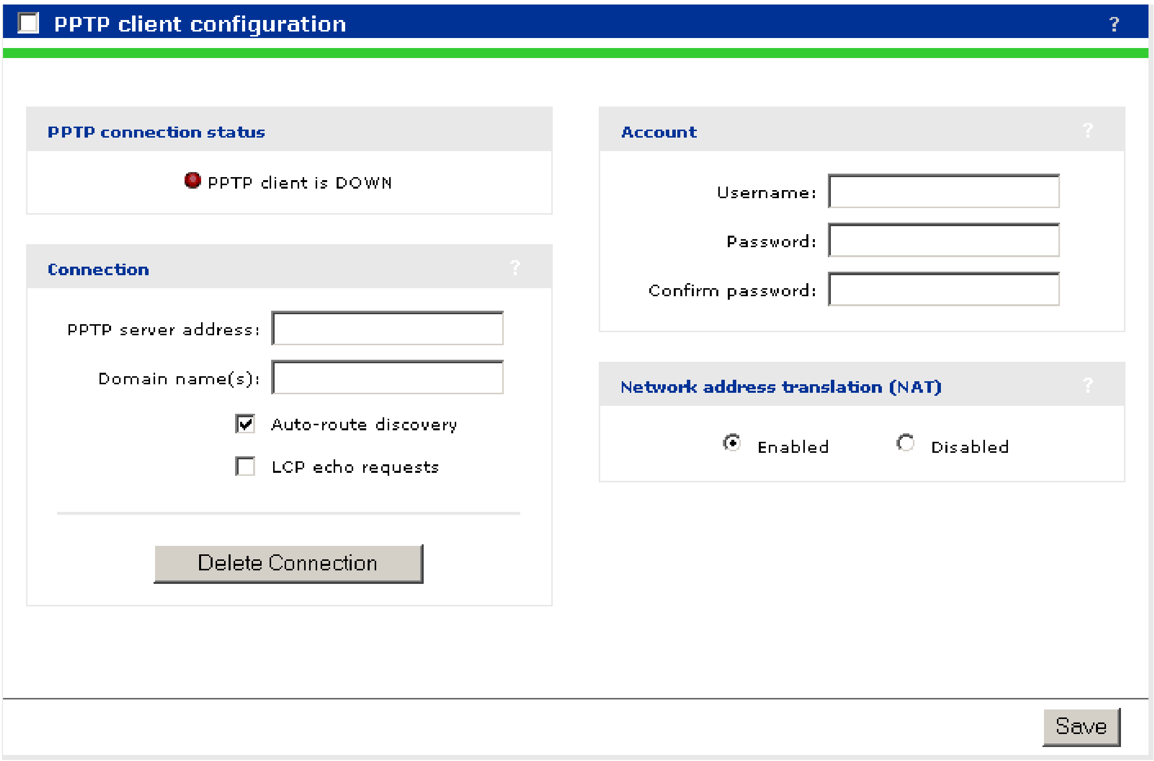
The PPTP client enables the service controller to create a secure tunnel to any device that provides a PPTP server. All traffic sent though this tunnel is protected against eavesdropping by means of encryption.

NOTE

The PPTP tunnel should not be used to transport user traffic. To prevent user traffic from entering the tunnel, you must define access list definitions to DENY access to all subnets on the other side of the tunnel. The tunnel should be used to carry management traffic only (RADIUS, SNMP, management sessions).

9.7.2 Configuration

To view and configure IPSec, select **Security** > **PPTP client**. The PPTP client is disabled by default.



□ PPTP client configuration ?

PPTP connection status

PPTP client is DOWN

Connection

PPTP server address:

Domain name(s):

☑ Auto-route discovery

□ LCP echo requests

Account

Username:

Password:

Confirm password:

Network address translation (NAT)

● Enabled ○ Disabled

Figure 9-14: PPTP Client Configuration

9.7.3 Configuration Settings

9.7.3.1 Connection

9.7.3.1.1 PPTP Server Address

Specify the domain name or IP address of the PPTP server the service controller will connect to.

9.7.3.1.2 Domain Name(s)

Specify the domain name(s) of the PPTP server. Put a space between each name as a separator. The service controller routes all traffic addressed to this domain through the PPTP connection.

9.7.3.1.3 Auto-route Discovery

Enable this option if you want the service controller to automatically discover and add routes to IP addresses on the other side of the PPTP tunnel. The addresses must be part of the specified domain. Routes are added only when an attempt is made to access the addresses.

9.7.3.1.4 LCP Echo Requests

Certain VPN servers may terminate your connection if it is idle. If you enable this option, the service controller will send a packet from time to time to keep the connection alive.

9.7.3.2 Account

9.7.3.2.1 Username

Specify the username the service controller will use to log on to the PPTP server. If you are logging on to a Windows NT domain, specify **domain_name\username**

9.7.3.2.2 Password / Confirm password

Specify the password the service controller will use to log on to the PPTP server.

9.7.3.3 Network Address Translation (NAT)

If you enable NAT, it effectively hides the addresses of all local computers so that they are not visible on the other side of the PPTP connection.

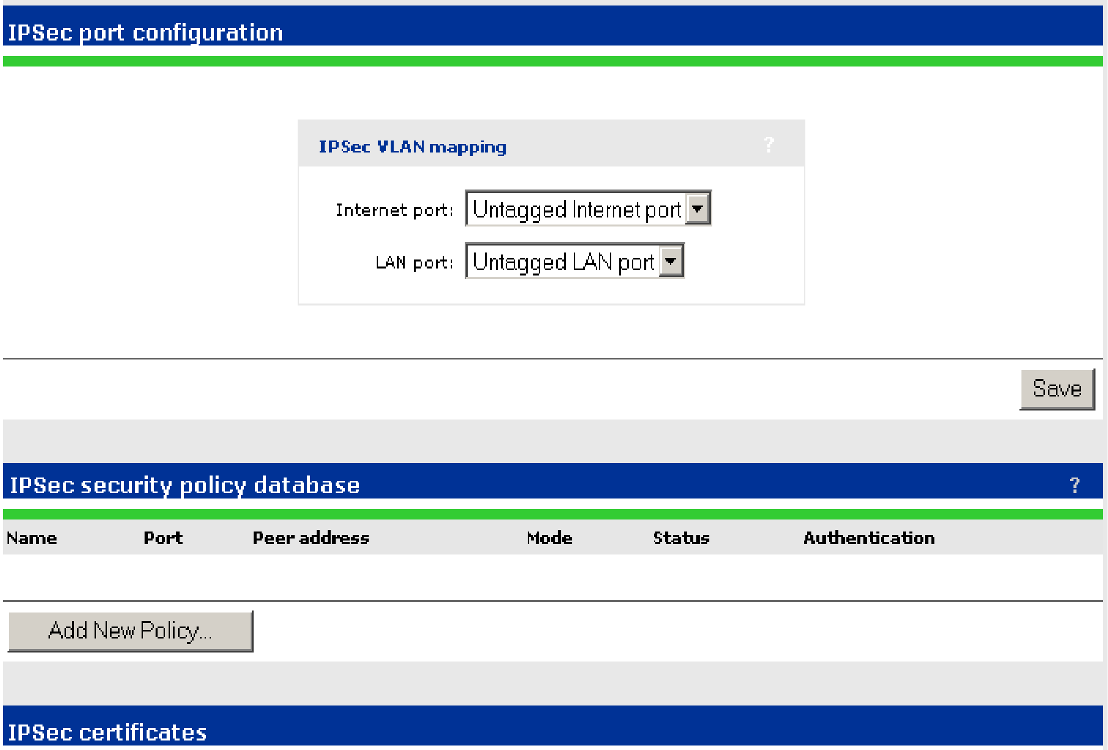
If you disable NAT, then the appropriate IP routes must be added to send traffic through the tunnel.

9.7.4 IPSec

IPSec provides the ability for two hosts (called peers in IPSec terminology) to communicate in complete security over any IP-based network. IPSec achieves this security though the use of sophisticated encryption that makes it impossible for an eavesdropper to decipher the transmitted data.

9.7.5 Configuration

To view and configure IPSec, select **Security > IPSec**. Initially, no security policies are defined.



IPSec port configuration

IPSec VLAN mapping

Internet port: Untagged Internet port

LAN port: Untagged LAN port

IPSec security policy database

Name	Port	Peer address	Mode	Status	Authentication

IPSec certificates

Figure 9-15: IPSec Port Configuration

To create a new policy select **Add New Policy**. See "Adding a New Security Policy" on page 241 for more information.

For information about the IPsec certificates section of this page, see "IPSec Certificates" on page 255.

9.7.6 Configuration Settings

9.7.6.1 IPSec VLAN Mapping

The **IPSec port configuration** page enables you to configure **IPSec VLAN mapping**. Use these settings to define how IPSec traffic is routed on the LAN and Internet ports. You can assign traffic to the untagged interface (no VLAN) or to any defined VLAN.

9.7.6.1.1 IPSec Security Policy Database

The **IPSec security policy database** table shows all the IPSec security policies that are defined on the service controller. A security policy defines the criteria that must be met for a peer to establish an IPSec security association (SA) with the service controller. Depending on its settings, a policy can allow one or more peers to establish an SA with the service controller. Each time an SA is established, a new entry is added to the IPSec security associations table. To view this table, select **Status** > **IPSec.**

The **IPSec security policy database** table shows the following fields from the IPSec policy database:

- **Name**: Name assigned to the security policy.
- **Port**: Port assigned to the security policy.
- **Peer address**: Address of the peer which can establish an SA using this policy.
- **Mode**: Indicates the IPSec mode (tunnel or transport) supported by this policy.
- **Status**: Indicates whether the policy has been enabled. An SA can only be established when a policy is enabled.
- **Authentication**: Indicates the method used to authenticate peers.

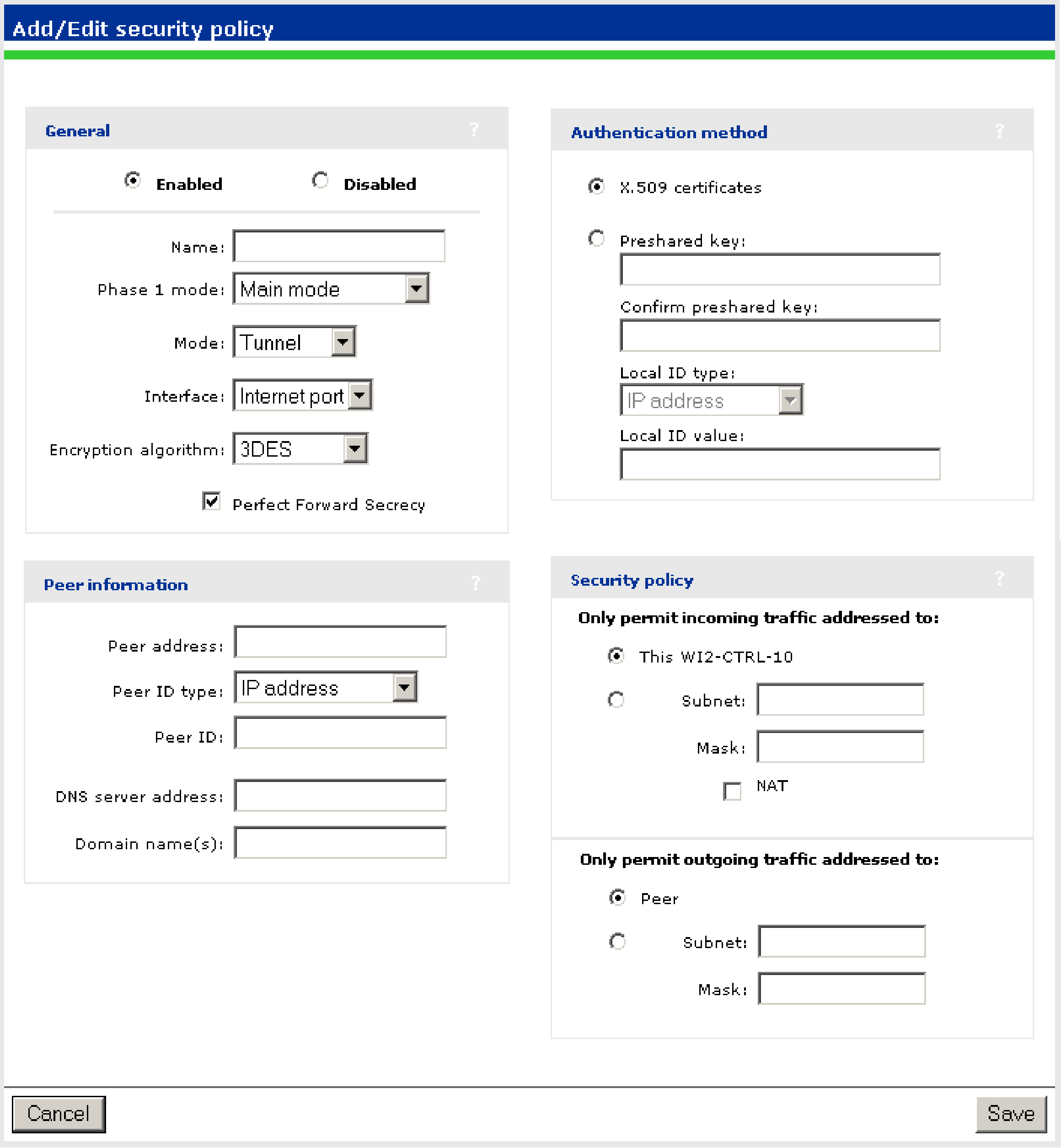
9.7.7 Adding a New Security Policy

A security association can be established between the service controller and a peer only if the policy is enabled.

The IPSec tunnel should not be used to transport user traffic. To prevent user traffic from entering the tunnel, you may need to define access list definitions to DENY access to all subnets on the other side of the tunnel (only if you set up the IPSec tunnel in "tunnel mode"). The tunnel should be used to carry management traffic only (RADIUS, SNMP, management sessions).

To add a new security policy, follow this procedure.

1. Select **Security** > **IPSec.** The **IPSec port configuration** page opens.
2. Select **Add New Policy.** The **Add/Edit security policy** page opens.



Add/Edit security policy

General

● Enabled ○ Disabled

Name:

Phase 1 mode: Main mode

Mode: Tunnel

Interface: Internet port

Encryption algorithm: 3DES

☑ Perfect Forward Secrecy

Authentication method

● X.509 certificates

○ Preshared key:

Confirm preshared key:

Local ID type: IP address

Local ID value:

Peer information

Peer address:

Peer ID type: IP address

Peer ID:

DNS server address:

Domain name(s):

Security policy

Only permit incoming traffic addressed to:

● This WI2-CTRL-10

○ Subnet:

Mask:

□ NAT

Only permit outgoing traffic addressed to:

● Peer

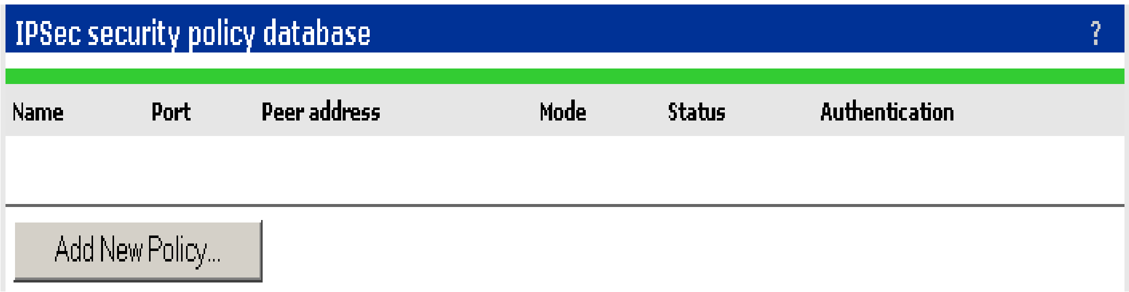
○ Subnet:

Mask:

Figure 9-16: Adding a New Security Policy

3 Configure the policy according to the information in the following sections: General Settings, Peer Information, Authentication Method, and Security Policy.

4 Select **Save**. The IPSec security policy database list is updated to include your new policy.



IPSec security policy database ?

Name	Port	Peer address	Mode	Status	Authentication

Figure 9-17: IPSec security policy database

5 You can now skip ahead to the next main section “Managing Certificates” on page 248.

9.7.7.1 General Settings

On the **Add/Edit security policy** page under **General,** you can configure the following parameters:

- **Enabled/ Disabled**: Select the appropriate radio button to enable or disable this security policy.
- **Name**: Specify a name that identifies the policy in the IPSec security policy database.
- **Phase 1 mode**: Select one of the following modes:
  - **Main mode**: This option is supported by most IPSec clients. It provides support for peer authentication via X.509 certificates or pre-shared keys.
  - **Aggressive mode**: Aggressive mode does not provide identity protection as main mode does. It is helpful when setting up a LAN-to-LAN tunnel when the Internet IP address is dynamic. The remote gateway can then use the group name to know which LAN-to-LAN tunnel to activate.
- **Mode**: Select one of the following modes of operation:
  - **Tunnel mode**: Use this mode if you want to create a secure tunnel to a remote peer to transfer data between two networks (i.e. both peers are operating as gateways). This option can also be used in peer-to-peer mode by selecting the appropriate options for Incoming traffic and Outgoing traffic.

- **Transport mode**: This option creates a point-to-point connection to a remote peer. Use this option if only the service controller needs to communicate with the remote peer.

- **Interface**: Select the port to which the policy applies.

- **Encryption algorithm**: Select the encryption algorithm used for this policy from the following choices:

  - **3DES**: A block cipher formed from the Data Encryption Standard (DES) cipher by using it three times. Also known as Triple DES.
  - **AES/3DES**: AES is the Advanced Encryption Standard (AES), also known as Rijndael, a block cipher adopted as an encryption standard by the US government.

- **Perfect Forward Secrecy**: Enable this checkbox to support automatic regeneration of keys. The key is changed according to the following intervals:

  - **Phase 1 exchange**: Key changed every 6 hours
  - **Phase 2 exchange**: Key changed every 1 hour

The service controller negotiates times up to 24 hours as required by the peer.

9.7.7.2 Peer Information

On the **Add/Edit security policy** page under **Peer information,** you can configure the following parameters:

- **Accept any peer**: (Available only in tunnel mode.) Enable this checkbox to permit the policy to accept an IPSec security association from any peer. When this option is enabled, the service controller sets ID type and ID automatically based on the selection for Authentication method. See IKE options for more information.

- **Peer address**: Specify the IP address or domain name of the peer.

- **Peer ID type**: Select the method used to identify the peer, as follows:

  - **IP address**: Specify the peer's IP address. If you are using a Preshared key for Authentication method, then you must use this option.

- **FQDN**: Specify a fully qualified domain name. For example, **gateway.mycompany.com**
- **user@FQDN**: Specify a fully-qualified user name. For example, **fred@mycompany.com**
- **DER_ASN1_DN**: Specify a distinguished name (DN) in LDAP (X.501) format. Specify a maximum of 91 characters. The following fields are supported:

Field	Description
CN	commonName
SN	serialNumber
C	countryName
L	localityName
ST	stateOrProvinceName
O	organizationName
OU	organizationalUnitName
G	givenName
E	emailAddress

Separate fields by a comma, space, or a forward slash (/). For example: (CN=joe/E=joe@company.com/O=Company Inc./C=US)

- **Peer ID**: Specify the peer ID based on the ID type you selected. If you selected IP address, you can leave this field blank to use the **Peer address.**
- **DNS server address**: Specify the domain name or IP address of the primary and secondary DNS servers that the service controller uses to resolve DNS requests related to the remote peer's domain. In most cases these servers are located on the network protected by the peer.
- **Domain name**: Specify the domain name of the peer. Any DNS requests on the wireless LAN for addressed to this domain are forwarded to the DNS server specified above. This enables the service controller to properly forward traffic to stations on the other side of an IPSec tunnel.

9.7.7.3 Authentication Method

On the **Add/Edit security policy** page under **Authentication method,** you can configure the following parameters:

- **X.509 certificates**: Select this option to use X.509 certificates to validate peers. To define certificate settings, select certificates on the security menu.
- **Preshared key**: Specify the key to be used by the service controller to validate peers. The service controller and the peer must both use the same key.
- **Confirm preshared key**: Re-enter the value of the preshared key.
- **Local ID type**: Select one of the following local ID types:
  - IP address
  - FQDN
  - user@FQDN
  - DER_ASN1_DN
- **Local ID value**: Specify the value for the chosen local ID type.

9.7.7.4 Security Policy

On the **Add/Edit security policy** page under **Security policy,** you can configure the following parameters:

- **Only permit incoming traffic addressed to**: These settings enable you to filter incoming traffic so that only traffic addressed to a specific network or network device is permitted from the peer. Note that the setting you make for this parameter must match the setting the peer makes for outgoing traffic. If not, the connection is not established.
  - **This** service controller: Accepts only incoming traffic that is addressed to the service controller. All other traffic is dropped.
  - **Subnet** and **Mask**: Accepts only incoming traffic that is addressed to the specified subnet or host. All other traffic is dropped. To accept all traffic from the peer, specify both the **Subnet** and **Mask** as **0.0.0.0**

  - **NAT**: Enable this checkbox to allow network address translation for traffic addressed to the specified **Subnet.** This hides the addresses of local computers from the peer. If you enable NAT, the peer does not have to match the settings for **Subnet.**

- **Only permit outgoing traffic addressed to**: These settings enable you to filter outgoing traffic so that only traffic addressed to the peer, a specific network, or network device is sent. All other traffic is sent onto the Internet outside the tunnel.

  Note that the setting you make for this parameter must match the setting the peer makes for incoming traffic. If not, the connection is not established.

  - **Peer**: Sends only outgoing traffic that is addressed to the peer. All other traffic is sent onto the Internet outside the tunnel.
  - **Subnet** and **Mask**: Sends only outgoing traffic that is addressed to the specified subnet or host. All other traffic is dropped. To send all outgoing traffic to the peer, specify both the **Subnet** and **Mask** as **0.0.0.0.**

9.8 Managing Certificates

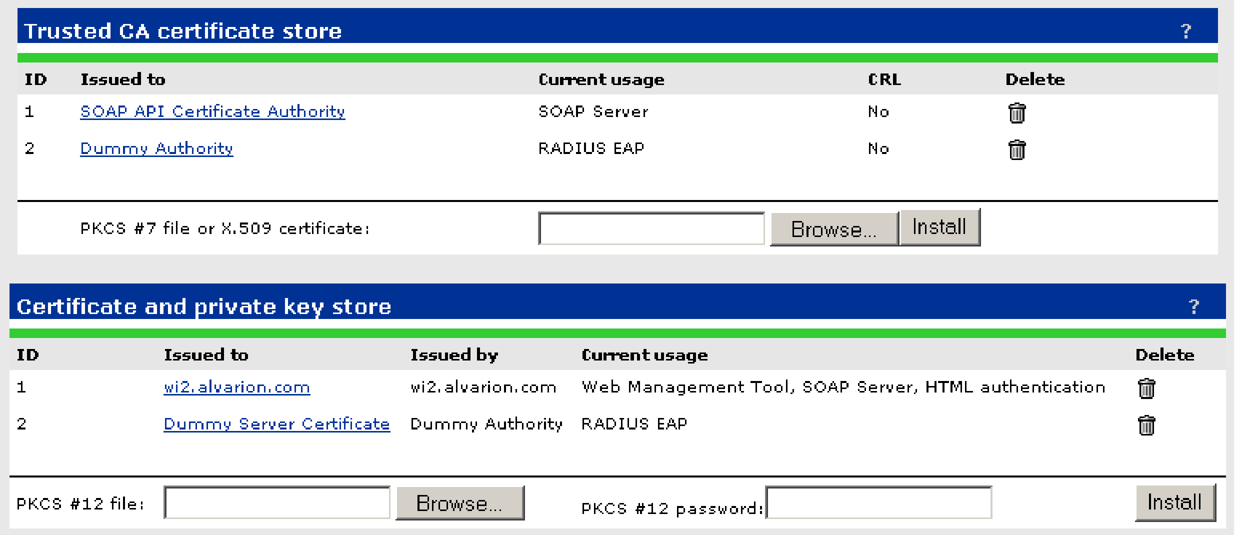
Digital certificates are electronic documents that are used to validate the end parties or entities involved in data transfer. These certificates are normally associated with X.509 public key certificates and are used to bind a public key to a recognized party for a specific time period.

Various features on the service controller make use of X.509 certificates for authentication and/or encryption of data exchanged with peers.

The service controller uses CA and SSL certificates for the authentication and/or encryption of data exchanged with peers. The following services make use of certificates:

- Administrators accessing the service controller’s management tool
- HTML users accessing the public access interface
- SOAP clients communicating with the service controller’s SOAP server
- RADIUS EAP-TLS
- RADIUS EAP-PEAP (server certificate only)
- IPSec connections
- NOC authentication (For details, see the *Network Access Admin Guide.*)

The certificate stores provide a repository for managing all certificates (except for those used by IPSec and NOC authentication). To view the certificate stores, select **Service Controller** >> **Security** > **Certificate stores**.



Trusted CA certificate store ?

ID	Issued to	Current usage	CRL	Delete
1	SOAP API Certificate Authority	SOAP Server	No	🗑
2	Dummy Authority	RADIUS EAP	No	🗑

PKCS #7 file or X.509 certificate: [ ] Browse... Install

Certificate and private key store ?

ID	Issued to	Issued by	Current usage	Delete
1	wi2.alvarion.com	wi2.alvarion.com	Web Management Tool, SOAP Server, HTML authentication	🗑
2	Dummy Server Certificate	Dummy Authority	RADIUS EAP	🗑

PKCS #12 file: [ ] Browse... PKCS #12 password: [ ] Install

Figure 9-18: Certificate Stores

9.8.1 Trusted CA Certificate Store

This list displays all root CA certificates installed on the service controller. The service controller uses the CA certificates to validate the certificates supplied by peers during authentication. Multiple CA certificates can be installed to support validation of peers with certificates issued by different CAs.

The service controller uses these certificates to validate certificates supplied by:

- Administrators accessing the service controller’s management tool
- HTML users accessing the public access interface
- SOAP clients communicating with the service controller’s SOAP server
- RADIUS EAP

Items provided in this list are as follows:

9.8.1.1 Issued to

Name of the certificate holder. Select the name to view the contents of the certificate.

9.8.1.2 Current usage

Lists the services that are currently using this certificate.

9.8.1.3 CRL

Indicates if a certificate revocation list is bound to the certificate. An X.509 certificate revocation list is a document produced by a certificate authority (CA) that provides a list of serial numbers of certificate that have been signed by the CA but that should be rejected.

9.8.1.4 Delete

Select to remove the certificate from the certificate store.

9.8.1.5 Installing a New CA Certificate

1. Specify the name of the certificate file or select **Browse** to choose from a list. CA certificates must be in X.509 or PKCS #7 format.
2. Select **Install** to install a new CA certificate.

9.8.1.6 CA Certificate Import Formats

The import mechanism supports importing the ASN.1 DER encoded X.509 certificate directly or as part of two other formats:

- PKCS #7 (widely used by Microsoft products)
- PEM, defined by OpenSSL (popular in the Unix world)
- The CRL can be imported as an ASN.1 DER encoded X.509 certificate revocation list directly or as part of a PEM file.

Content and file format	Items carried in the file	Description
ASN.1 DER encoded X.509 certificate	One X.509 certificate	This is the most basic format supported, the certificate without any envelope.
X.509 certificate in PKCS #7 file	One X.509 certificate	Popular format with Microsoft products.
X.509 certificate in PEM file	One or more X.509 certificates	Popular format in the Unix world. X.509 DER certificate is base64 encoded and placed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines. Multiple certificates can be repeated in the same file.

Content and file format	Items carried in the file	Description
ASN.1 DER encoded X.509 CRL	One X.509 CRL	Most basic format supported for CRL.
X.509 CRL in PEM file	One X.509 CRL	Same format as X.509 certificate in PEM format, except that the lines contain BEGIN CRL and END CRL.

9.8.1.7 Default CA Certificates

The following certificates are installed by default:

- **SOAP API Certificate Authority:** Before allowing a SOAP client to connect the service controller checks the certificate supplied by a SOAP client to ensure that it is issued by a trusted certificate authority (CA).

- **Dummy Authority:** Used by the internal RADIUS server. You should replace this with your own CA certificate.

NOTE

For security reasons, you should replace the default certificates with your own.

9.8.2 Certificate and Private Key Store

This list displays all certificates installed on the service controller. The service controller uses these certificates and private keys to authenticate itself to peers.

Items provided in this list are as follows:

9.8.2.1 Issued to

Name of the certificate holder. Select the name to view the contents of the certificate.

9.8.2.2 Issued by

Name of the CA that issued the certificate.

9.8.2.3 Current Usage

Lists the services that are currently using this certificate.

9.8.2.4 Delete

Select to remove the certificate from the certificate store.

9.8.2.5 Installing a New Private Key/Public Key Certificate Chain Pair

NOTE

RADIUS EAP certificates must have the X.509 extensions. Information about this is available in the Microsoft knowledgebase at:
http://support.microsoft.com/kb/814394/en-us

The certificate you install must:

- Be in PKCS #12 format.
- Contain a private key (a password controls access to the private key).
- Not have a name that is an IP address. The name should be a domain name containing at least one dot. If you try to add a certificate with an invalid name, the default certificate is restored.

The common name in the certificate is automatically assigned as the domain name of the service controller.

1. Specify the name of the certificate file or select **Browse** to choose one from a list. Certificates must be in PKCS #7 format.
2. Specify the **PKCS #12 password**.
3. Select **Install** to install the certificate.

9.8.2.6 Default Installed Private Key/Public Key Certificate Chains

The following private key/public key certificate chains are installed by default:

- **wireless.alvarion.com:** Default certificate used by the management tool, SOAP server, and HTML-based authentication.
- **Dummy Server Certificate:** Used by the internal RADIUS server. This certificate is present only to allow EAP-PEAP to work if the client chooses not to verify the server's certificate. You should replace this with your own certificate for maximum security.

NOTE

When a web browser connects to the service controller using SSL, the service controller sends only its own SSL certificate to the browser. This means that if the certificate has been signed by an intermediate certificate authority, and if the web browser only knows about the root certificate authority that signed the public key certificate of the intermediate certificate authority, the web browser does not get the whole certificate chain it needs to validate the identity of the service controller.

Consequently, the web browser issues security warnings.

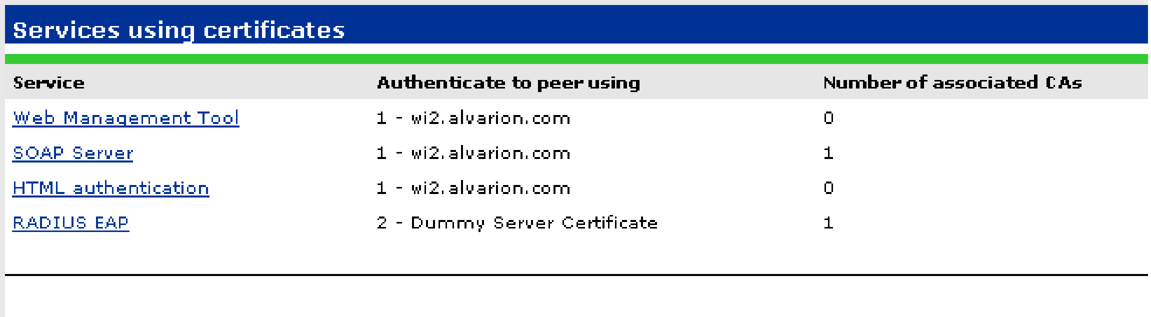
To avoid this problem, make sure that you install the entire certificate chain when you install a new certificate on the service controller.

NOTE

An SNMP trap is sent to let you know when the service controller's SSL certificate is about to expire if you enable the **Traps** option on the **Service Controller >> Management > SNMP** page and then click **Configure traps** and enable the **Certificate about to expire trap** option under **Maintenance**.

9.8.3 Certificate Usage

To see the services that are associated with each certificate, select **Security > Certificate usage**. With the factory default certificates installed, the page will look like this:



Services using certificates

Service	Authenticate to peer using	Number of associated CAs
Web Management Tool	1 - wi2.alvarion.com	0
SOAP Server	1 - wi2.alvarion.com	1
HTML authentication	1 - wi2.alvarion.com	0
RADIUS EAP	2 - Dummy Server Certificate	1

Figure 9-19: Certificate Usage

9.8.3.1 Service

Name of the service that is using the certificate. To view detailed information on the certificate select the service name.

9.8.3.2 Authenticate to Peer Using

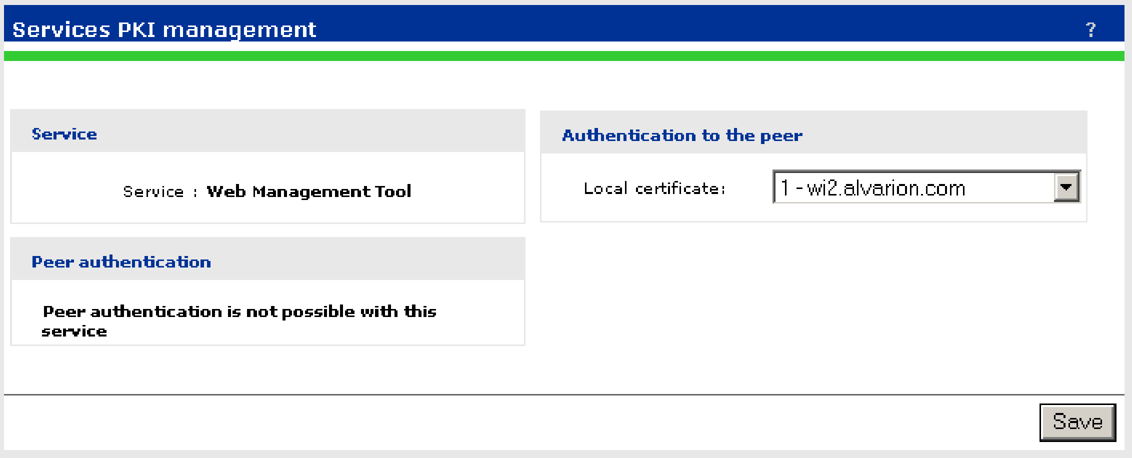
Name of the certificate and private key. The service controller is able to prove that it has the private key corresponding to the public key in the certificate. This is what establishes the service controller as a legitimate user of the certificate.

9.8.3.3 Number of Associated CAs

Number of CA certificates used by the service.

9.8.3.4 Changing the Certificate Assigned to a Service.

Select the service name to open the Certificate details page. For example, if you select **Web** management tool, you will see:



Services PKI management

Service

Service : Web Management Tool

Authentication to the peer

Local certificate: 1 - wi2.alvarion.com

Peer authentication

Peer authentication is not possible with this service

Figure 9-20: Service PKI Management

Under **Authentication to the peer**, select a new **Local certificate** and then select **Save**.

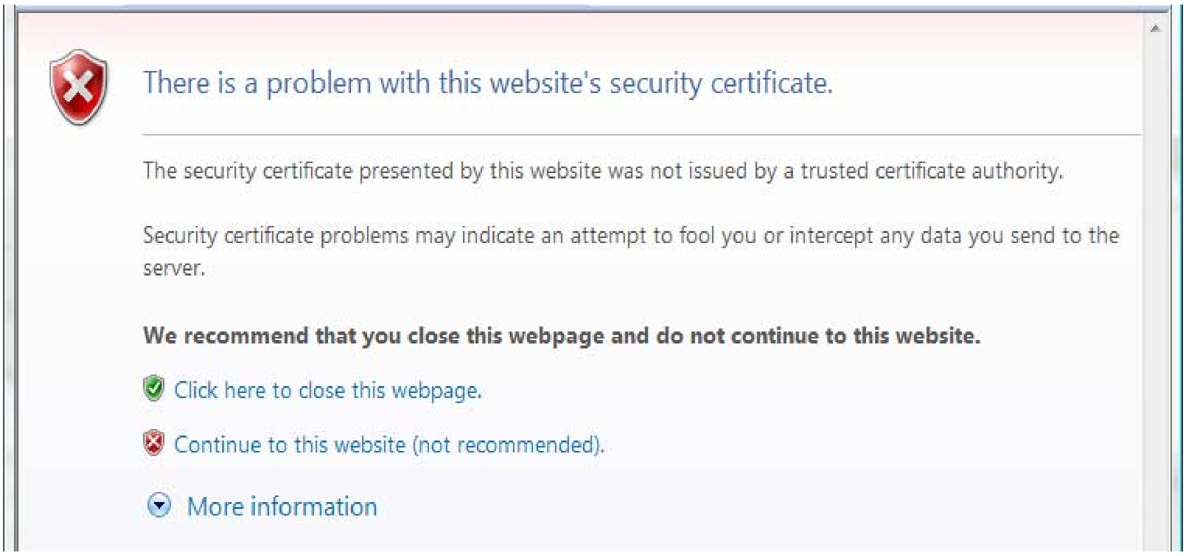
9.8.4 About Certificate Warnings

Access to the management tool and the public access interface Login page must occur through a secure connection (SSL). Until a valid, trusted certificate is installed, certificate warnings will appear at login.

To continue to work with the management tool without installing a certificate, proceed as follows: At the security certificate prompt, in Microsoft Internet Explorer 7, select **Continue to this website**; in Firefox 2, select **Accept this certificate temporarily for this session** and **OK**.

To eliminate these warnings you can purchase a valid SSL certificate (from a source such as Verisign) that will work with the default configuration of your web browser, and install it on the service controller.

The following is an example of a security warning displayed by Internet Explorer 7.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

Figure 9-21: Certificate Warnings

9.8.5 IPSec Certificates

IPSec certificates are managed on the lower portion of the **Service Controller** >> **Security** > **IPSec** page.

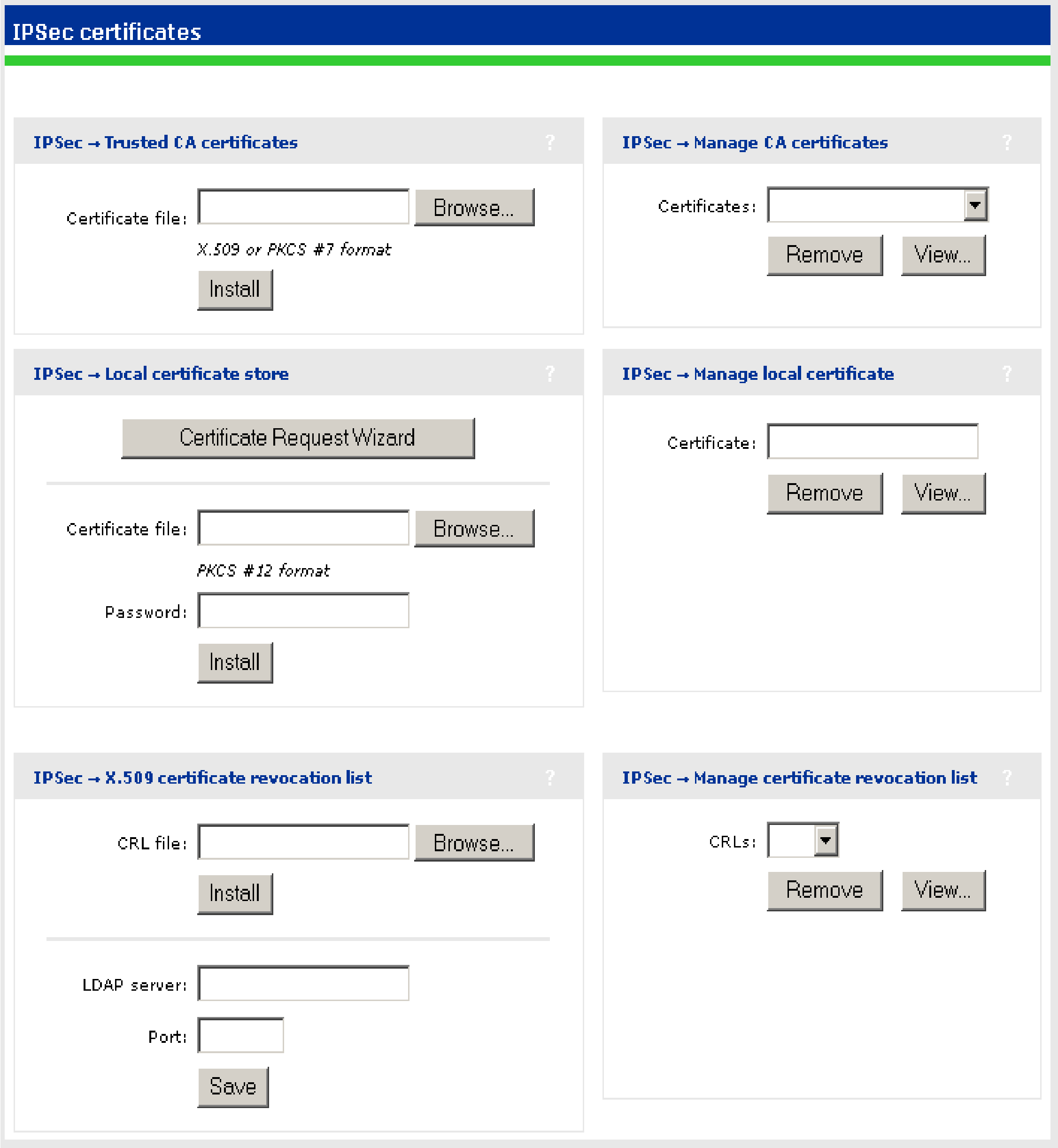


Figure 9-22: IPSec Certificates

9.8.5.1 IPSec — Trusted CA Certificates

The service controller uses the CA certificates to validate the certificates supplied by peers during the authentication process. Multiple CA certificates can be installed to support validation of peers with certificates issued by different CAs.

- **Certificate file**: Specify the name of the certificate file or select **Browse** to choose from a list. CA certificates must be in X.509 or PKCS #7 format.

- **Install**: Select to install the specified certificate.

9.8.5.2 IPSec — Manage CA Certificates

Use this box to manage the root CA certificate.

- **Certificate**: Select from a list of installed certificates.
- **Remove**: Delete the item shown under **Certificate.**
- **View**: Open the item shown under **Certificate** for viewing.

9.8.5.3 IPSec — Local Certificate Store

This is the certificate that the service controller uses to identify itself to IPSec peers.

NOTE

If the local certificate includes a CA certificate, both certificates are installed.

- **Certificate Request Wizard**: Helps you to generate a certificate request that can be used to obtain a signed certificate from a certificate authority. Once you obtain the certificate, you can use the **Certificate Request Wizard** to install it on the service controller.
- **Certificate file**: Specify the name of the certificate file or select **Browse** to choose from a list.
- **Password**: Specify the certificate password.
- **Install**: Select to install the certificate.

9.8.5.4 IPSec — Manage Local Certificate

Use this box to manage the local certificate.

- **Certificate**: Shows the common name of the installed certificate.
- **Remove**: Delete the item shown under **Certificate.**
- **View**: Open the item shown under **Certificate** for viewing.

9.8.5.5 IPSec — X.509 Certificate Revocation List

Use this box to update the certificate revocation list (CRL) that is issued by the certificate authority.

The service controller uses the CRL to determine if the certificates provided by clients during the authentication process have been revoked. The service controller will not establish a security association with a client that submits a revoked certificate.

The service controller can obtain a CRL in two ways:

- You can manually install it.
- The service controller can automatically install a CRL based on information contained in a client certificate. This occurs only if a CRL is not installed, or if the installed CRL is expired.
- **CRL file**: Specify the name of the CRL file or select **Browse** to choose from a list.
- **Install**: Select to install the specified CRL.
- **LDAP server**: A client certificate may contain a list of locations where the CRL can automatically be retrieved. This location may be specified as an HTTP URL, FTP URL, LDAP URL, or LDAP directory. If the LDAP URL or directory is incomplete, the service controller uses the location you specify to resolve the request. Incomplete HTTP or FTP URLs fail.
- **Port**: Port on the LDAP server. Default is 389.

9.8.5.6 IPSec — Manage Certificate Revocation List

Use this box to manage the CRL.

- **CRLs**: Shows a list of installed certificate revocation lists.
- **Remove**: Deletes the item shown under **CRLs.**
- **View**: Opens the item shown under **CRLs** for viewing.

10

Chapter 10 - User Authentication

In This Chapter:

10.1 Key Concepts

NOTE

This chapter discusses user authentication as it applies to controlled APs only. For information on working with autonomous APs, see "Working with Autonomous APs" on page 325.

User authentication tasks can be handled either by the AP or by the service controller. This is controlled by the settings of the access control and authentication options set on the virtual network to which a user is assigned. Refer section "About Access Control And Authentication" on page 100.

10.1.1 Authentication Support on the Service Controller

The following authentication types are supported on the service controller for both wired and wireless clients (except where noted):

- WPA / WPA2 (wireless users only)
- 802.1X (Wired 802.1x users can only be supported on the default virtual network profile if access control is enabled. Wired 802.1x users on a VLAN can be supported on any virtual network profile as long as access control is enabled and the appropriate VLAN is defined as the VSC ingress.)
- MAC (wireless users only)
- HTML (Wired HTML-based users can only be supported on the default VSC profile if access control is enabled. Wired HTML-based users on a VLAN can be supported on any VSC profile as long as access control is enabled and the appropriate VLAN is defined as the VSC ingress.)

The service controller can validate user login credentials using the local user list (integrated RADIUS server), a third-party RADIUS server, or an external Active Directory service. For information on configuring these options:

Authentication server	See
Integrated RADIUS server	"Locally-defined User Accounts" on page 266 "Using the Integrated RADIUS Server" on page 212
Third-party RADIUS server	"Using a Third-party RADIUS Server" on page 216
Active Directory	"Using an Active Directory Server" on page 222

10.1.2 Authentication Support on a Controlled AP

The following authentication types are supported on a controlled AP for wireless clients only:

- WPA / WPA2
- 802.1X
- MAC

The AP can validate user login credentials using either the service controller or a third-party RADIUS server. Access-controlled virtual networks always use the service controller for all user authentication tasks.

10.1.3 Authentication Types

10.1.3.1 WPA / WPA2 and 802.1X Authentication

Full support is provided for users with 802.1X or WPA / WPA2 client software, and 802.1X client software that uses the following:

- EAP-TLS: Extensible Authentication Protocol Transport Layer Security.
- EAP-TTLS: Extensible Authentication Protocol Tunnelled Transport Layer Security.
- EAP-SIM: Extensible Authentication Protocol Subscriber Identity Module.
- PEAP: Protected Extensible Authentication Protocol.

The group key can be changed at a specific interval.

NOTE

For security reasons, use of 802.1X without enabling dynamic WEP encryption is not recommended.

10.1.3.2 MAC-based Authentication

Devices can be authenticated based on their MAC address. This is useful for authenticating devices that do not have a web browser (cash registers, for example). As soon as the devices's MAC address appears on the network, the service controller (or AP) attempts to authenticate them.

There are two types of MAC-based authentication: global MAC and virtual network-based MAC.

Global MAC	VSC-based MAC
Supported on the service controller only.	Supported on both service controller and AP.
Applies to both wired and wireless client stations.	Applies to wireless client stations only.
Applies to all virtual networks that have HTML-based user authentication enabled. Authentication server is defined on a per-virtual network basis however.	Customizable on a per-virtual network basis.

User credentials can be validated using either a local user accounts, a third-party RADIUS server, or Active Directory. If more than one option is active, the local accounts are always checked first.

10.1.3.2.1 Global MAC

You can define global MAC-based authentication settings using the Alvarion-AVPair value string `mac-address`, which you must add to the RADIUS account for the service controller. Refer to the *Network Access Admin Guide* for configuration details.

Although the global MAC-based authentication settings apply to all all virtual networks that have HTML-based user authentication enabled, each virtual network can use a different authentication server to validate user credentials. To define an authentication server for each virtual network, open the **Add/Edit Virtual Service Community** page and use the **HTML-based user logins** box to select the authentication method.

10.1.3.2.2 Virtual Network-based MAC

Each virtual network can have a unique settings for media access control (MAC) authentication of wireless client stations. Support for RADIUS accounting is also configurable for each virtual network. See “Working with Virtual Networks” on page 97.

10.1.3.3 HTML-based Authentication

This option provides support for users to log in with a web browser via the public access interface provided by the service controller.

10.1.3.3.1 No Authentication

For applications where a remote device performs all authentication functions, it can be useful to disable authentication on the service controller and instead, forward all traffic on a virtual network into an egress GRE tunnel or egress VLAN for authentication by the remote device.

The *Deployment Guide* contains scenarios that illustrate this type of setup.

10.1.3.4 Using More than One Authentication Type in a Virtual Network

For added flexibility, you can enable both the 802.1X and virtual network-based MAC authentication at the same time. The following table shows the results for all authentication scenarios.

NOTE

MAC authentication always takes place first. If it fails, 802.1X is then attempted.

Active Authentication Method	Authentication result		Network Access?
	MAC	**802.1X**	
MAC	Failure	-	No
	Success	-	Yes
802.1X optional	-	Success	Yes
	-	Failure	No
	-	-	Yes
802.1X mandatory	-	Failure	No
	-	Success	Yes
	-	-	No

Active Authentication Method	Authentication result		Network Access?
	MAC	802.1X	
MAC optional + 802.1X optional	Failure	-	No
		Success	Yes
		Failure	No
	Success	Failure	No
		-	Yes
		Success	Yes
MAC optional + 802.1X mandatory	Failure	-	No
		Success	Yes
		Failure	No
	Success	Failure	No
		-	No
		Success	Yes
MAC mandatory+ 802.1X optional	Failure	-	No
		Success	No
		Failure	No
	Success	Failure	No
		-	Yes
		Success	Yes
MAC mandatory+ 802.1X mandatory	Failure	-	No
		Success	No
		Failure	No
	Success	Failure	No
		-	No
		Success	Yes

10.1.3.4.1 Authentication Examples

10.1.3.4.1.1 MAC and 802.1X enabled, mandatory 802.1X authentication disabled

Wireless client stations are automatically authenticated by their MAC address.

- **If MAC authentication succeeds,** the client station gains access. Next, the client station can initiate an 802.1X session, causing 802.1X authentication to take place. The result of this authentication then takes precedence over the MAC authentication result.

- ***(When MAC mandatory disabled.)*** **If MAC authentication fails,** the client station does not gain access but can still initiate an 802.1X session, causing 802.1X authentication to take place. If the result of this authentication is successful, then the client station gains access.

- *(When MAC mandatory enabled.)* **If MAC authentication fails,** the client station does not gain access regardless of the 802.1X result.

10.1.3.4.1.2 MAC and 802.1X Enabled, Mandatory 802.1X Authentication Enabled

Wireless client stations are automatically authenticated by their MAC address. If MAC authentication succeeds they do not gain access until 802.1X authentication is successful.

10.1.3.4.1.3 MAC disabled and 802.1X Enabled, Mandatory 802.1X Authentication Disabled

Wireless client stations automatically gain access to the network with no authentication required. If the client station starts an 802.1X session, authentication takes place. If the result of this authentication is failure, then the client station looses access to the network.

10.1.3.4.1.4 MAC Disabled and 802.1X Enabled, Mandatory 802.1X Authentication Enabled

Wireless client stations gain access to the network only after successful 802.1X authentication.

10.1.3.5 FIlters

Input filters are available that enable you to control wireless access based on the IP or MAC address of client stations. These filters are configurable at the virtual network level.

For information see

- “Wireless MAC Filter” on page 116

- “Wireless IP Filter” on page 117

10.2 Locally-defined User Accounts

The service controller provides support for locally-defined user accounts with a wide range of customizable options. Locally-defined user accounts use the integrated RADIUS server. Configuration of these accounts is done using the options on the **Service Controller >> Users** menu, which includes the following configuration pages: User accounts, Account profiles, Subscription plans, and Session persistence.

Each user account:

- Obtains account properties from one or more **account profiles**.
- Obtains account durations from one or more **subscription plans**.
- Is restricted for use with one or more **virtual networks**.

10.2.1 Features

10.2.1.1 Access Control

Two types of local user accounts are available: access-controlled and not access-controlled.

- Access-controlled accounts must be used with a virtual network that is configured to provide access control.
- Non access-controlled accounts must be used with a virtual network that is *not* configured to provide access control. These accounts are used to handle authentication directly at the AP and cannot not involve the access control capabilities of the service controller (the service controller must not be in the traffic data path).

10.2.1.2 Validity and Subscription Plans

Each user account can be associated with a subscription plan that defines:

- The time period during which the account is available.
- The total amount of time a user can be online when logged in with the account.

10.2.1.3 Virtual Network Usage

User accounts can be restricted to specific virtual networks. if a the specified virtual network is not available, then the user will not be able to connect with the account.

10.2.1.4 Account Profiles

An account profile is used to define a specific set of features for a user account. Multiple account profiles can be applied to a user account allowing the feature sets of each profile to be added to the account.

NOTE

Each profile that is applied to a user account must have a unique feature set. The same feature cannot be present in two different profiles.

10.2.1.4.1 About the Default AC Profile

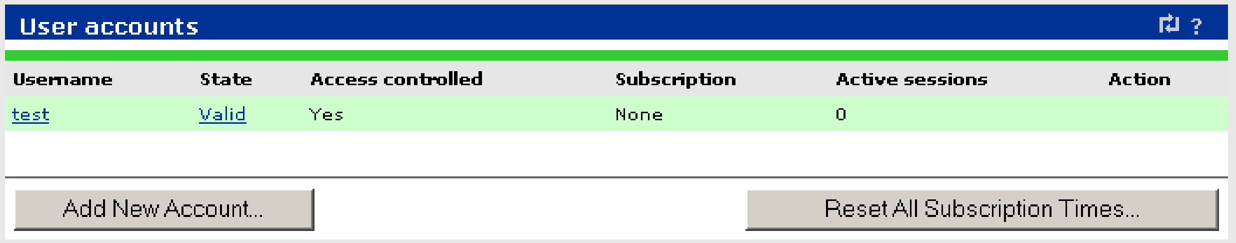
The **Default AC** profile is created by the service controller and is always applied to all user accounts. It provides access to the values of any user-applicable attributes that are defined on the
Service Controller >> **Public access** > **Attributes** page, and includes attributes retrieved from a RADIUS server or configured attributes. For example, the **Default AC** profile provides access to the values of the following service controller attributes (if defined):

- DEFAULT-USER-ACCT-INTERIM-UPDATE
- DEFAULT-USER-MAX-INPUT-PACKETS
- DEFAULT-USER-MAX-OUTPUT-PACKETS
- DEFAULT-USER-MAX-TOTAL-PACKETS
- DEFAULT-USER-MAX-INPUT-OCTETS
- DEFAULT-USER-MAX-OUTPUT-OCTETS
- DEFAULT-USER-MAX-TOTAL-OCTETS
- DEFAULT-USER-IDLE-TIMEOUT
- DEFAULT-USER-SMTP-REDIRECT

- DEFAULT-USER-SESSION-TIMEOUT
- DEFAULT-USER-ONE-TO-ONE-NAT

10.2.2 Defining a User Account

1 Select **Service Controller >> Users > User accounts**. This User accounts page opens. It presents a list of all defined user accounts. Initially this list will be empty.

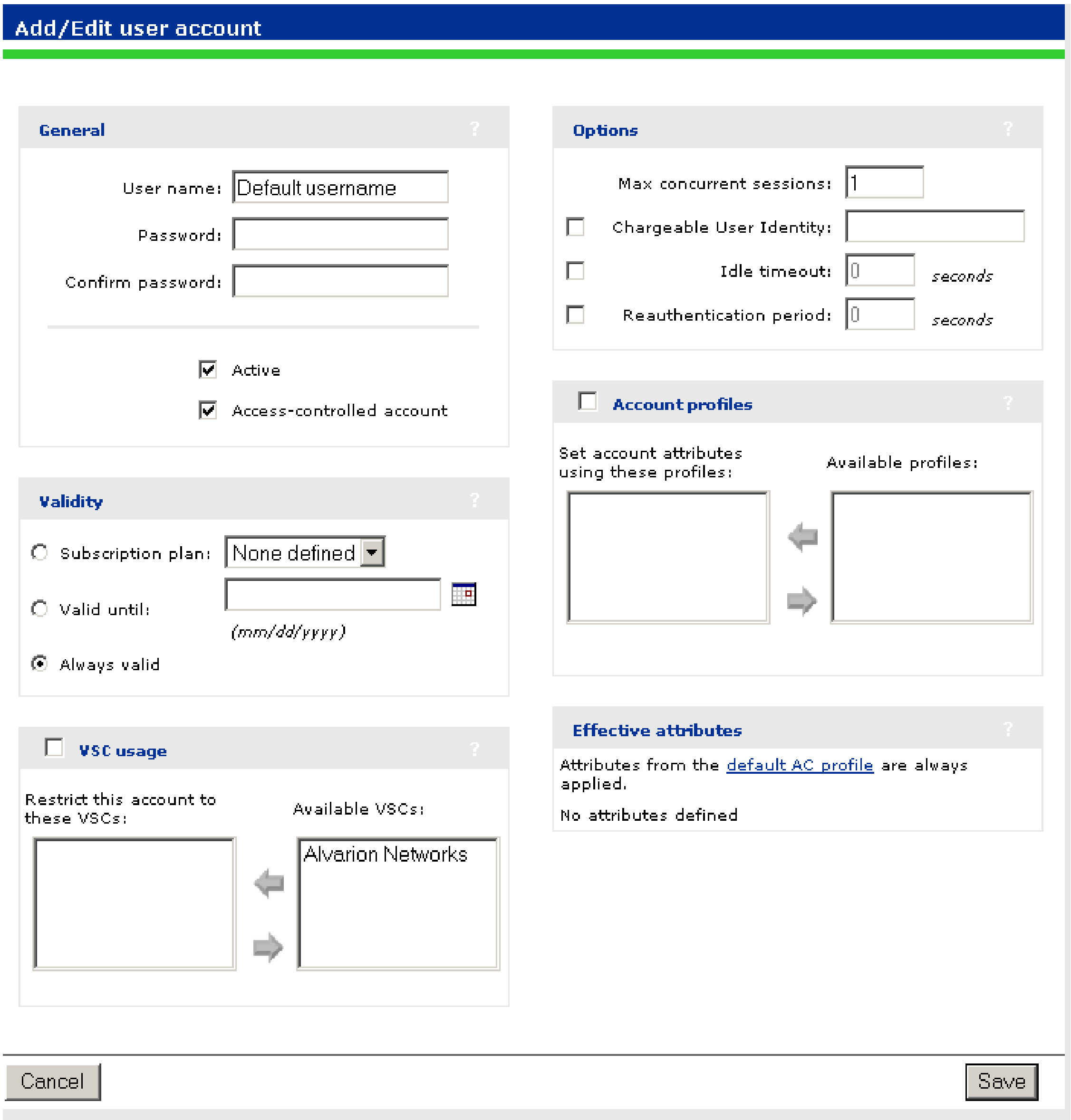


User accounts

Username	State	Access controlled	Subscription	Active sessions	Action
test	Valid	Yes	None	0	

Figure 10-1: Defining a User Account

2 Select **Add New Account**. The Add/Edit user accounts page opens.



Add/Edit user account

General

User name: Default username

Password:

Confirm password:

☑ Active

☑ Access-controlled account

Validity

○ Subscription plan: None defined

○ Valid until: (mm/dd/yyyy)

● Always valid

□ **VSC usage**

Restrict this account to these VSCs:

Available VSCs: Alvarion Networks

Options

Max concurrent sessions: 1

□ Chargeable User Identity:

□ Idle timeout: 0 *seconds*

□ Reauthentication period: 0 *seconds*

□ **Account profiles**

Set account attributes using these profiles:

Available profiles:

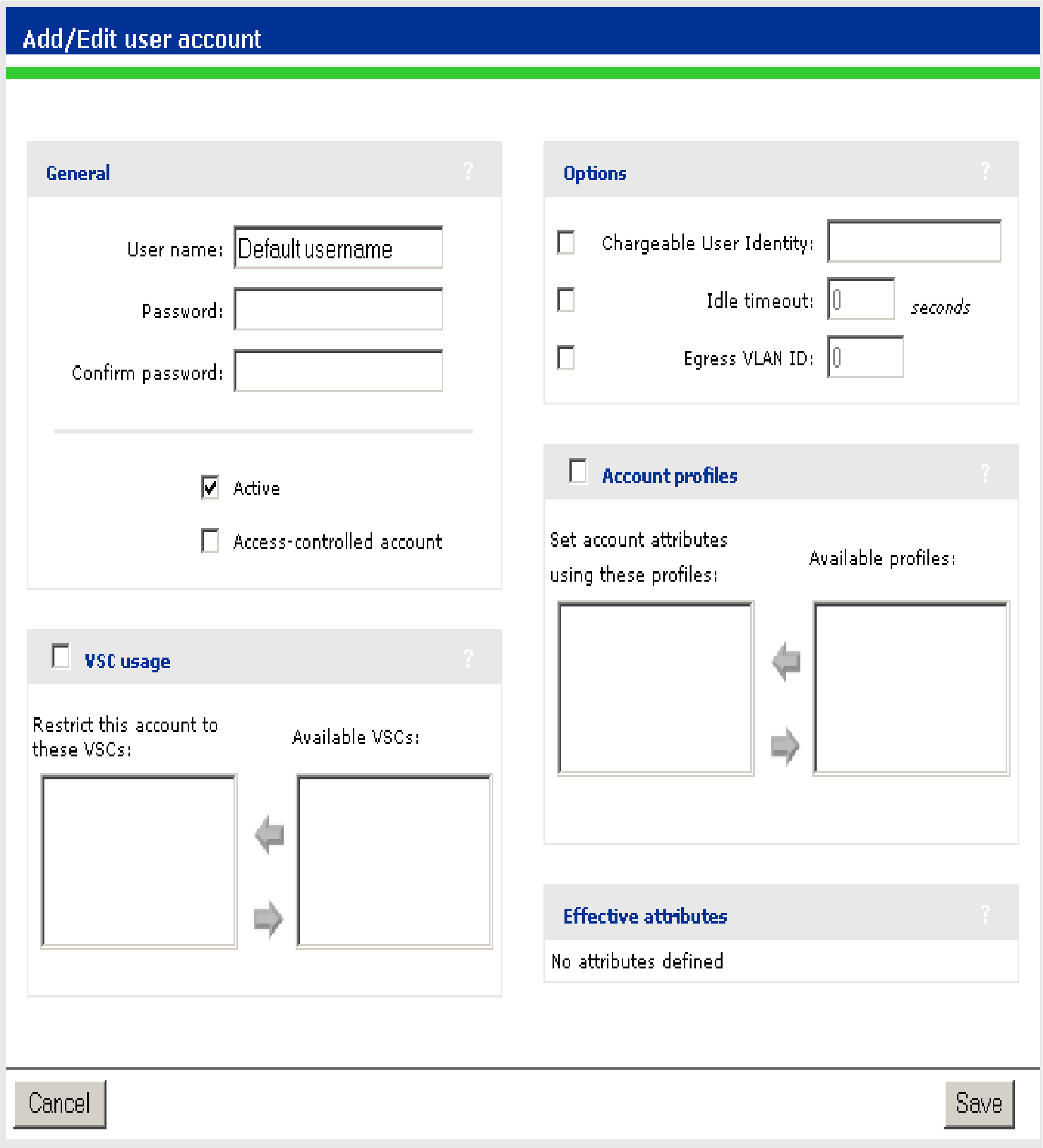
Effective attributes

Attributes from the default AC profile are always applied.

No attributes defined

Figure 10-2: Add/Edit User Account

If you disable the Access-controlled account option, the page will look like this:



Add/Edit user account

General

User name: Default username

Password:

Confirm password:

☑ Active

□ Access-controlled account

□ VSC usage

Restrict this account to these VSCs:

Available VSCs:

Options

□ Chargeable User Identity:

□ Idle timeout: 0 *seconds*

□ Egress VLAN ID: 0

□ Account profiles

Set account attributes using these profiles:

Available profiles:

Effective attributes

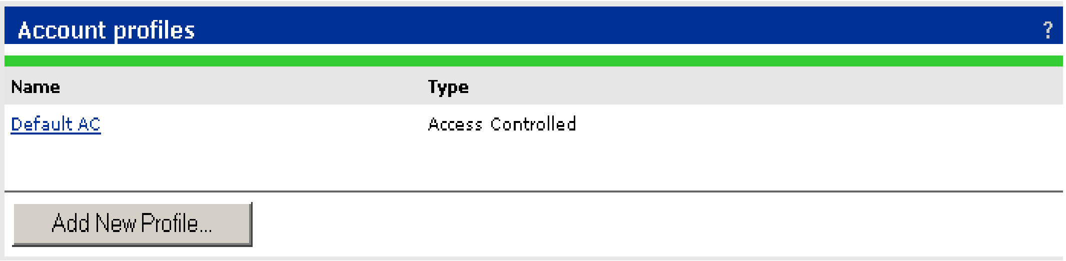
No attributes defined

Figure 10-3: Add/Edit User Account with Access Controlled Account Disabled

3 Configure account options as described in the online help.

10.2.3 Defining Account Profiles

1 Select **Service Controller** >> **Users** > **Account profiles**. This Account profiles page opens. It presents a list of all defined profiles. Initially this list will contain the profile **Default AC**.

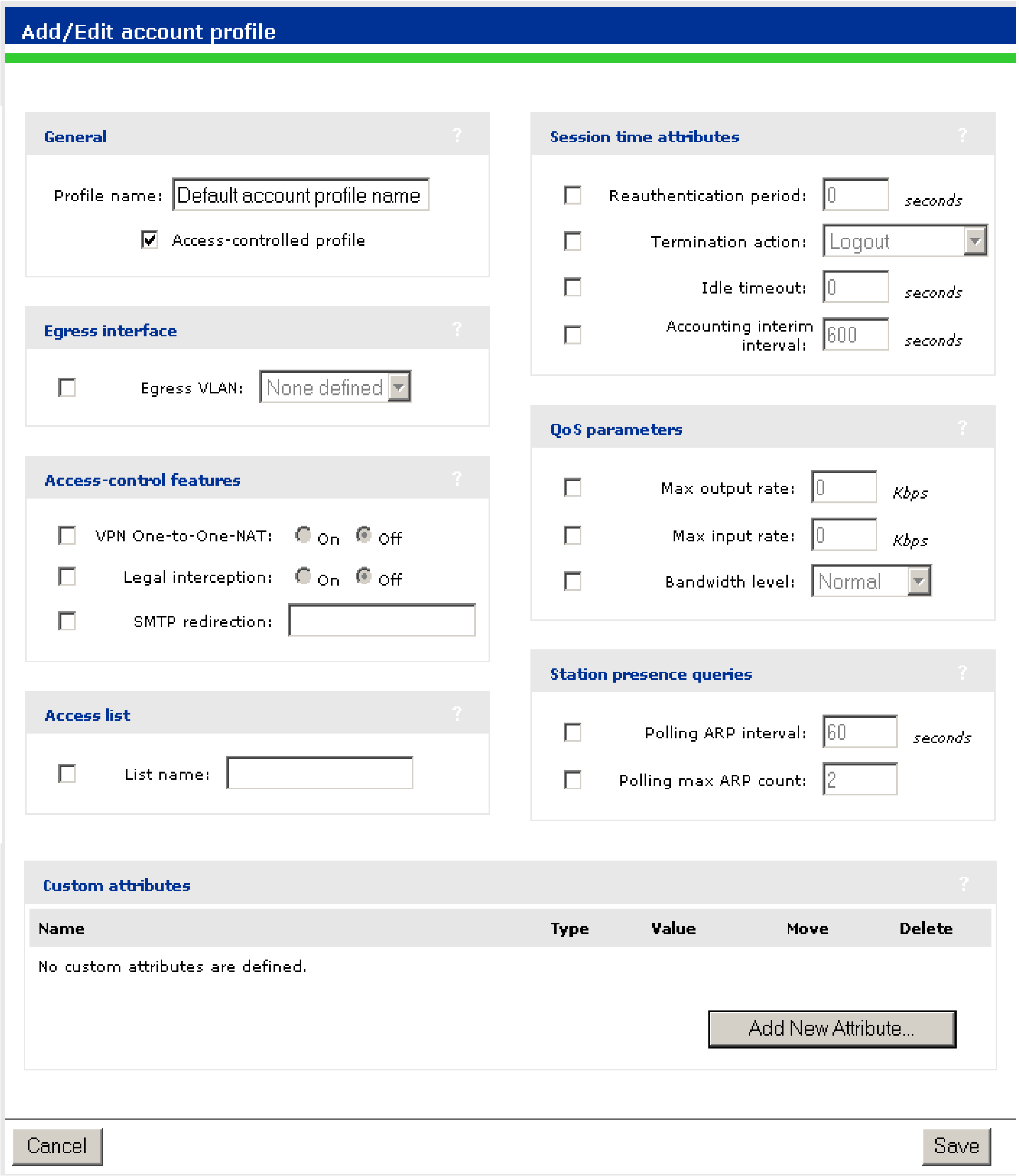


Account profiles

Name	Type
Default AC	Access Controlled

Figure 10-4: Defining Account Profiles

2 Select **Add New Profile**. The Add/Edit account profile page opens.



Add/Edit account profile

General

Profile name: Default account profile name

☑ Access-controlled profile

Egress interface

□ Egress VLAN: None defined

Access-control features

□ VPN One-to-One-NAT: ○ On ● Off

□ Legal interception: ○ On ● Off

□ SMTP redirection:

Access list

□ List name:

Session time attributes

□ Reauthentication period: 0 seconds

□ Termination action: Logout

□ Idle timeout: 0 seconds

□ Accounting interim interval: 600 seconds

QoS parameters

□ Max output rate: 0 Kbps

□ Max input rate: 0 Kbps

□ Bandwidth level: Normal

Station presence queries

□ Polling ARP interval: 60 seconds

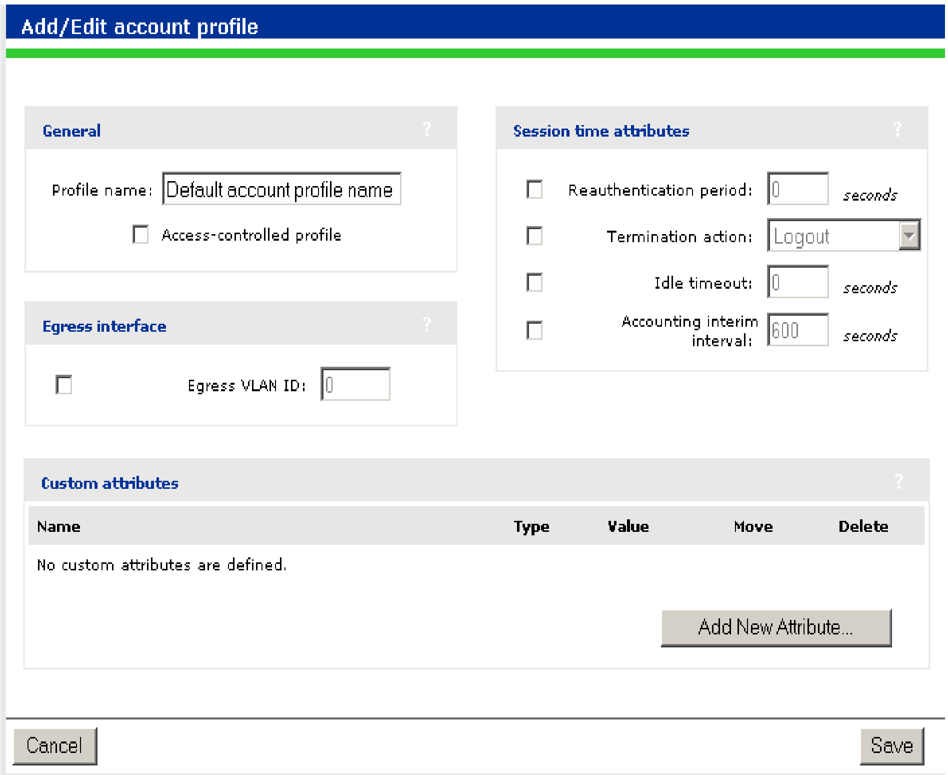
□ Polling max ARP count: 2

Custom attributes

Name	Type	Value	Move	Delete
No custom attributes are defined.				

Figure 10-5: Add/Edit Account Profile

If you disable the Access-controlled account option, the page will look like this:



Add/Edit account profile

General

Profile name: Default account profile name

□ Access-controlled profile

Egress interface

□ Egress VLAN ID: 0

Session time attributes

□ Reauthentication period: 0 seconds

□ Termination action: Logout

□ Idle timeout: 0 seconds

□ Accounting interim interval: 600 seconds

Custom attributes

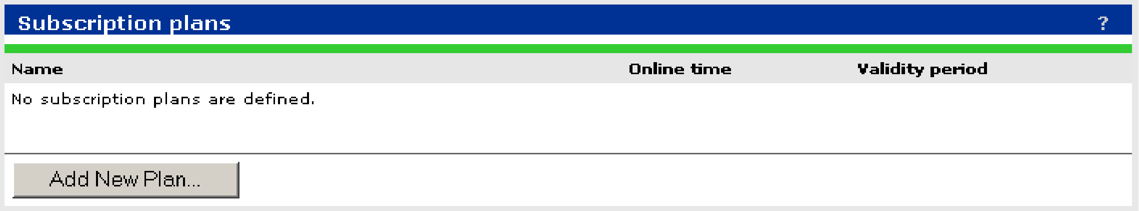
Name	Type	Value	Move	Delete
No custom attributes are defined.				

Figure 10-6: Add/Edit Account Profile with Access Controlled Account Disabled

3 Configure profile options as described in the online help.

10.2.4 Defining Subscription Plans

1 Select **Service Controller** >> **Users** > **Subscription plans**. This Subscription plans page opens. It presents a list of all defined subscription plans. Initially this list will be empty.

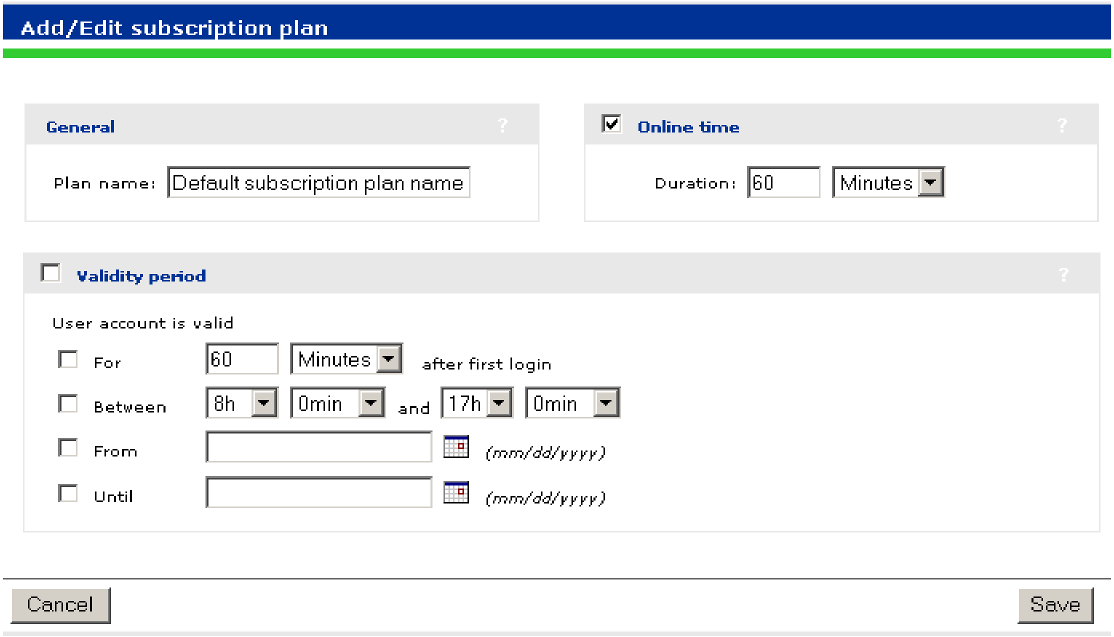


Subscription plans

Name	Online time	Validity period
No subscription plans are defined.		

Figure 10-7: Defining Subscription Plans

2 Select **Add New Plan**. The Add/Edit subscription plan page opens.



Add/Edit subscription plan

General

Plan name: Default subscription plan name

☑ Online time

Duration: 60 Minutes

☐ Validity period

User account is valid

☐ For 60 Minutes after first login

☐ Between 8h 0min and 17h 0min

☐ From (mm/dd/yyyy)

☐ Until (mm/dd/yyyy)

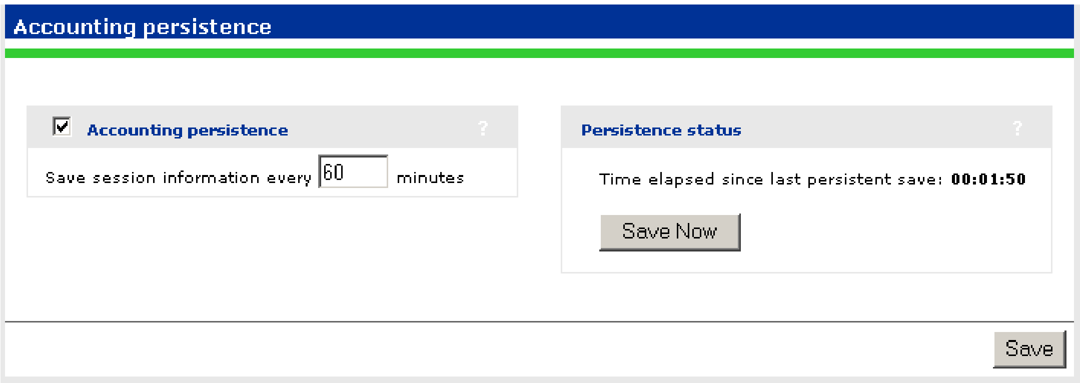
Figure 10-8: Add/Edit a Subscription Plan

3 Configure profile options as described in the online help.

10.2.5 Accounting Persistence

Enable this option to have the service controller save accounting information to its internal flash memory so that can be recovered in case of abnormal system shutdown. Restarting the service controller via its management tool (**Service Controller** >> **Maintenance** > **System**) saves before restarting.

The minimum save time is 30 minutes.



Accounting persistence

☑ Accounting persistence

Save session information every 60 minutes

Persistence status

Time elapsed since last persistent save: **00:01:50**

Figure 10-9: Accounting Persistence

11

Chapter 11 - Public/Guest Network Access

In This Chapter:

11.1 Key Concepts

TIP

For detailed information on configuring the public/guest network access feature, see the Network Access Admin Guide.

The *Public/Guest Network Access* feature enables the service controller to provide controlled network access for a variety of deployments. Some common applications of this feature are:

- Providing Internet access to wireless customers in airports, restaurants, train stations, conference halls, etc.
- Providing wireless and wireline access to staff and guests in hospitals, corporations, government buildings.
- Providing wireless and wireline access to students, staff, and teachers in schools and universities.
- Providing outdoor wireless access for an entire town, enabling city workers, police, fire, public security, and the general public to connect.

This chapter provides an overview of the public/guest network access feature and how it can be used. For detailed configuration information, see the *Network Access Admin Guide.*

11.1.1 About the Public and Protected Networks

In this type of deployment, the service controller acts as the gatekeeper between between two distinct network segments: the public network and the protected network.

- Typically, access to the public network and its resources is available to all users once they successfully associate with the wireless network.
- Access to the private network is restricted by the service controller, and typically requires that users be authenticated by the service controller. In most cases this occurs using a web browser to access the public access interface Login page.

The following diagram shows the public and private networks for a simple public access deployment.

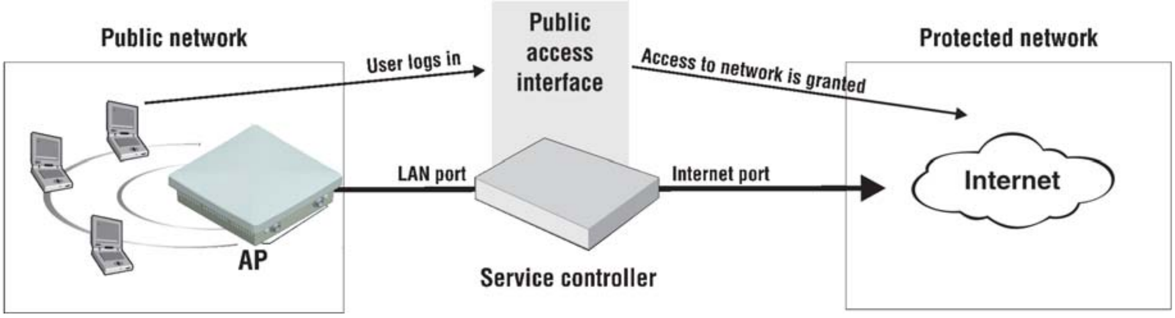


Figure 11-1: Public and Private Networks for a Simple Public Access Deployment

The service controller does not have to physically separate the two networks. Data traffic can be controlled using VLANs and/or data tunnels. For example:

11.1.1.1 Default Setup

needs to describe user access, site list, html interface that is active by default on the alvarion networks virtual network

Me think that you discovered a bug in the documentation. The documentation should have stated that the access is limited by default to the login page as long as you have an authentication enabled on the given virtual network. And even more, MAC-Auth as configured in the virtual network only support wireless devices meaning that if you enable MAC-Auth and you also have wired clients, those gain network access.

11.1.2 Configuration

Configuration of the public/guest network access feature can be separated into the following areas:

- **User access:** Defines the protected network resources that a user is able to access before and after being authenticated, support for connecting users configured with static IP addresses and HTTP proxy servers, and MAC authentication.

- **Session properties:** Defines settings for features that are provided on user sessions, such as email redirection, bandwidth limits, idle timeout, and traffic quotas.

- **Public access interface:** Defines settings that control the public access interface, which is a set of web pages that provide users with the ability to log in, log out, and view the status of their wireless connections to the public access network. The service controller enables you to tailor the public access interface web pages to provide a customized look-and-feel for your public access site.

11.1.2.1 Configuring the Features

Configuration of the features occurs via either configuration options on the service controller's management tool, or via RADIUS attributes. RADIUS attributes can be defined locally on the service controller, or in a RADIUS account. Attributes are available for user-related features (defined in user accounts) and site-related features (defined in a site account).

The following table summaries how to configure the features.

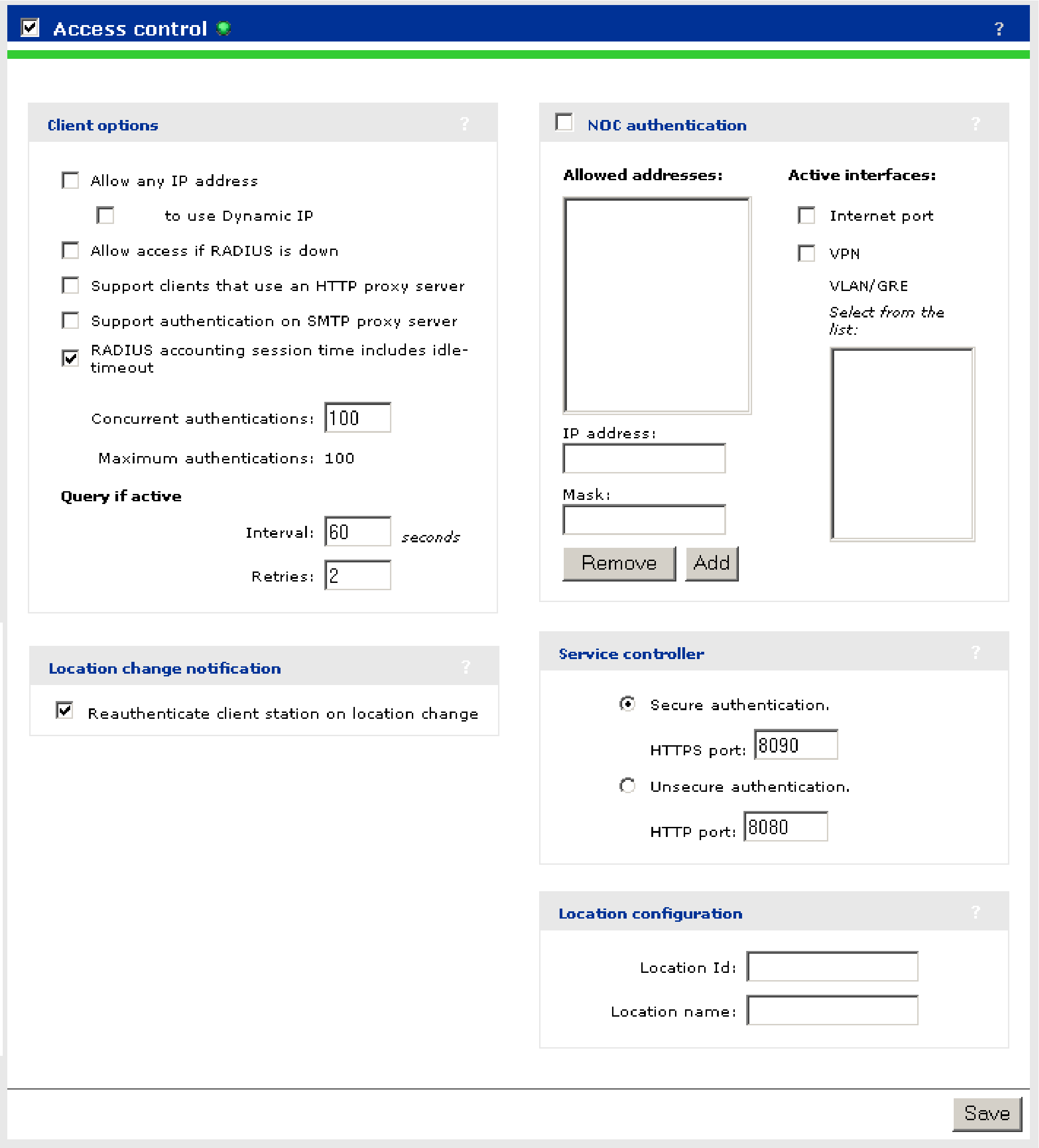
Feature	Description	See . . .
User access	Enable the **HTML-user logins** option in a virtual network to present the public access interface login page to users. Alternately, you can enable support for MAC authentication or WPA/802.1X. In this case users do not need to login via HTML.	"Virtual Network Configuration Options" on page 105
	Enable support for static IP addresses and HTTP proxy users and other client access features.	"Global Access Control Settings" on page 280
Session properties	Define default session properties for all users using RADIUS attributes, either directly on the service controller, or in an account on a third-party RADIUS server.	"Attributes" on page 286 *Network Access Admin Guide*
	Define properties for individual users via the local user accounts.	"Locally-defined User Accounts" on page 266
	Define properties for individual users via the RADIUS accounts.	*Network Access Admin Guide*
	Define properties for individual users via the Active Directory accounts.	"Using an Active Directory Server" on page 222

Feature	Description	See . . .
Public/guest network access interface	To support the public/guest network access feature on a virtual network, the virtual network must have access control enabled.	"Virtual Network Configuration Options" on page 105
	Define default session properties for all users by setting RADIUS attributes, either directly on the service controller, or in an account on a third-party RADIUS server.	*Network Access Admin Guide*
	Define properties for individual users via the local user accounts.	"Locally-defined User Accounts" on page 266

11.2 Global Access Control Settings

The access control mechanism enables the service controller to manage user access to protected network resources. The features provided by the access control mechanism are only supported on virtual networks that are configured for access control.

Support for access control must be enabled and disabled individually for each virtual network. Select **Public access** > **Access control** to configure global settings.



☑ Access control

Client options

□ Allow any IP address

□ to use Dynamic IP

□ Allow access if RADIUS is down

□ Support clients that use an HTTP proxy server

□ Support authentication on SMTP proxy server

☑ RADIUS accounting session time includes idle-timeout

Concurrent authentications: 100

Maximum authentications: 100

Query if active

Interval: 60 *seconds*

Retries: 2

Location change notification

☑ Reauthenticate client station on location change

□ **NOC authentication**

Allowed addresses:

IP address:

Mask:

Active interfaces:

□ Internet port

□ VPN

VLAN/GRE

Select from the list:

Service controller

● Secure authentication.

HTTPS port: 8090

○ Unsecure authentication.

HTTP port: 8080

Location configuration

Location Id:

Location name:

Figure 11-2: Global Access Control Settings

11.2.1 Client Options

Client options settings apply to wireless client stations that are authenticated by the service controller.

- **Allow any IP address:** Enable this option to allow client stations with static IP addresses that are not on the same subnet as the service controller to connect to the service controller. This permits users to access the network without reconfiguring their network settings.

- For example, by default the service controller creates a network on the subnet 192.168.1.0. A client station that is preconfigured with the address 10.10.4.99 can connect to the service controller without changing addresses.

- **to use Dynamic IP:** Enable this option to provide network address translation for client stations with static IP addresses. This permits the service controller to assign an alias address to the client that puts it on the same subnet as the virtual network the client is associated with.

NOTE

This option cannot be used if NAT is enabled on the Internet port.

- **Allow access if RADIUS is down:** Enable this option to allow users associated with a virtual network that uses a RADIUS server for HTML authentication to automatically authenticate when the RADIUS server is down or unreachable. Once the RADIUS server is available again, free user sessions remain active until the user logs out.

NOTE

This does not apply to users using 802.1X, WPA / WPA2, or MAC, where available.

- **Support clients that use an HTTP proxy server:** Enable this option to allow the service controller to support client stations that use a proxy server for HTTP and HTTPS, without reconfiguration of the client stations.

  Ensure that client stations:

  - Do not use a proxy server on ports 21, 23, 25, 110, 443, 8080, or 8090; to support ports 8080 and 8090, change the settings under **Access controller ports.**
  - Use the same proxy server address and port number for both HTTP and HTTPS.

- **Support authentication on SMTP proxy server:** Enable this option to allow the service controller to supply a username and password for the user to authenticate with the SMTP proxy server. You can define the username and password in the RADIUS account for the service controller or for the user.

- **RADIUS accounting session time includes idle time-out:** Enable this checkbox to specify that the service controller includes the idle time-out in the total session time for a client station when reporting to a RADIUS server. Disable this checkbox to remove the idle time-out from the total session time.

- **Concurrent authentications:** Specify the number of authentication sessions that can be active on the service controller at any one time.

- **Query if active:** The service controller continually polls authenticated client stations to ensure that they are active. If no response is received and the number of retries is reached, the client station is disconnected. To use this feature, client stations must have L2 connectivity to the service controller.

  This feature enables the service controller to detect if two client stations are using the same IP address but have different MAC addresses. If this occurs, access is terminated for this IP address removing both stations from the network.

  Changing these values may have security implications. A large interval provides a greater opportunity for a session to be hijacked.

  - **Interval:** Specify how long to wait between polls.

  - **Retries:** Specify how many polls a client station can fail to reply to before it is disconnected.

11.2.2 Location Change Notification

- **Reauthenticate client stations on location change:** When this option is enabled, the service controller will automatically reauthenticate users via third-party RADIUS server when they switch to:

- a wireless cell with a different SSID

- a different VLAN ID on the same virtual network

- an AP with a different MAC address

- an AP with a different group name

- different wireless mode (802.11b/g)

NOTE

Location change notification is not supported for locally authenticated users.

11.2.3 NOC Authentication

Enable the **NOC authentication** checkbox to support network operations center authentication. For a detailed discussion of this feature, refer to the *Network Access Admin Guide*. NOC authentication must be used in conjunction with the remote login page feature. The remote login page feature enables users to be redirected to a remote web server instead of using the internal login page on the service controller.

To authenticate users, the remote server collects user information and sends it to the service controller, which in turn forwards it to a RADIUS server.

- **Allowed addresses:** The service controller accepts user authentication requests only from the IP addresses in this list. When the list is empty, the service controller accepts authentication requests from any address.

- **Active interfaces:** Select the interface(s) on which the service controller can accept authentication requests.

11.2.4 Service Controller Ports

Select the protocol and port that will be used for HTML-based logins to the public access interface.

- If you select secure authentication, users will be redirected to the login page using HTTPS on the specified port.

- If you select unsecure authentication, users will be redirected to the login page using HTTP on the specified port.

If you enable support for proxy settings under **Client options**, you must change the selected port to support client stations that are using proxy servers on the standard port (8080 or 8090). The following mappings are recommended:

- Map the secure port 8090 to 444

- Map the unsecure port 8080 to 81

Make sure that you do not remap these ports to values already in use on your network.

11.2.5 Location Configuration

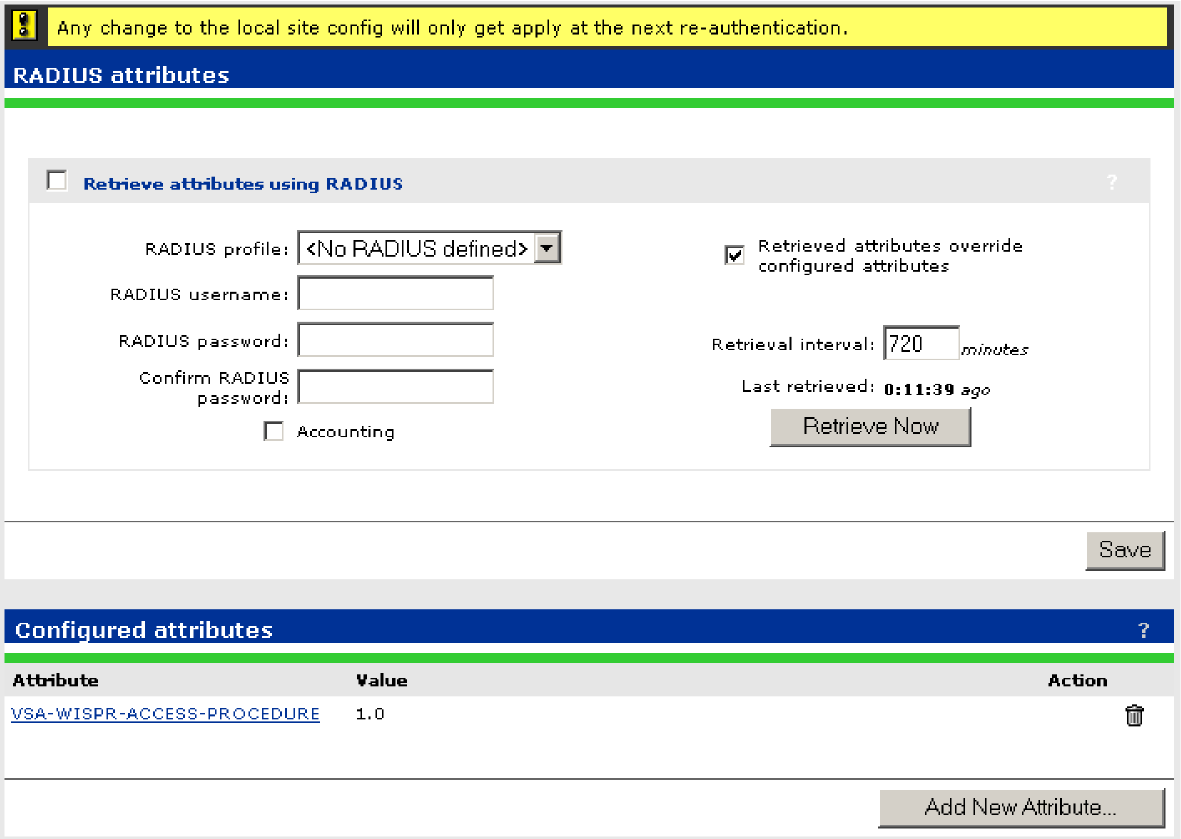
Location configuration values are returned to IPass clients and are sent in RADIUS authentication Access Requests and Accounting Requests for all users authenticated by this service controller.

- **Location Id:** Specify the Wireless ISP Roaming (WISPr) location ID assigned to the service controller.
- **Location name:** Specify the WISPr location name assigned to the service controller.

11.3 Attributes

RADIUS attributes are used to define a number of features of the public access interface. Attributes can be retrieved from a third-party RADIUS server of defined directly on the service controller. For more information on these attributes refer to the *Network Access Admin Guide.*

Select **Public Access** > **Attributes** to open the **RADIUS Attributes** page.



Any change to the local site config will only get apply at the next re-authentication.

RADIUS attributes

□ Retrieve attributes using RADIUS

RADIUS profile:	<No RADIUS defined>	☑ Retrieved attributes override configured attributes	
RADIUS username:			
RADIUS password:		Retrieval interval:	720 minutes
Confirm RADIUS password:		Last retrieved:	0:11:39 ago
□ Accounting			

Configured attributes

Attribute	Value	Action
VSA-WISPR-ACCESS-PROCEDURE	1.0	🗑

Figure 11-3: Radius Attributes

Configurable parameters on the **RADIUS Attributes** page include those described in the following sections.

11.3.1 Retrieve Attributes Using RADIUS

If you enable this option, the service controller will use the services of a RADIUS server to retrieve configuration settings for customization of the public access interface. The settings must be defined in a RADIUS account for the service controller.

The retrieved settings will be added to those defined in the **Configured attributes** table (if any) to build the complete list of defined attributes. If the same attribute is defined on both the RADIUS server and in the Configured attributes table, the setting of **Retrieved attributes override configured attributes** determines which setting is used.

Enable the **Retrieve attributes using RADIUS** checkbox to configure the following parameters:

- **RADIUS profile**: Select a previously configured RADIUS profile to use to authenticate the service controller.
- **RADIUS username**: Specify the username of the RADIUS account assigned to the service controller.
- **RADIUS password / Confirm password**: Specify the password of the RADIUS account assigned to the service controller.
- **Accounting**: Enable this option to have the service controller generate a RADIUS accounting request ON/OFF each time its authentication state changes.
- **Retrieved attributes override configured attributes**: Enable this option to have attributes retrieved from the RADIUS server overwrite settings defined in the **Configured attributes** table.
- **Retrieval interval**: Specify the number of minutes to use for a retrieval interval. The service controller retrieves configuration settings each time this interval expires. This enables the service controller to retrieve updated operating information at regular intervals.
- **Last retrieved**: Shows the amount of time that has passed since the service controller successfully authenticated.

  To avoid potential service interruptions that may occur when new operating information is activated by the service controller, it is strongly recommends that you use a large interval (12 hours or more).

  You can override this value using the RADIUS attribute Session-timeout, which enables the following effective strategy: Configure Retrieval interval to a small value (10 to 20 minutes) and set the RADIUS attribute Session-timeout to override it with a large value (12 hours) when authentication is successful. Since the Retrieval interval is also respected for Access Reject packets, this configuration results in a short reauthentication interval in the case of failure, and a long one in the case of success.

- **Retrieve Now**: Select to force the service controller to contact the RADIUS server and retrieve configuration settings.

11.3.2 Configured Attributes

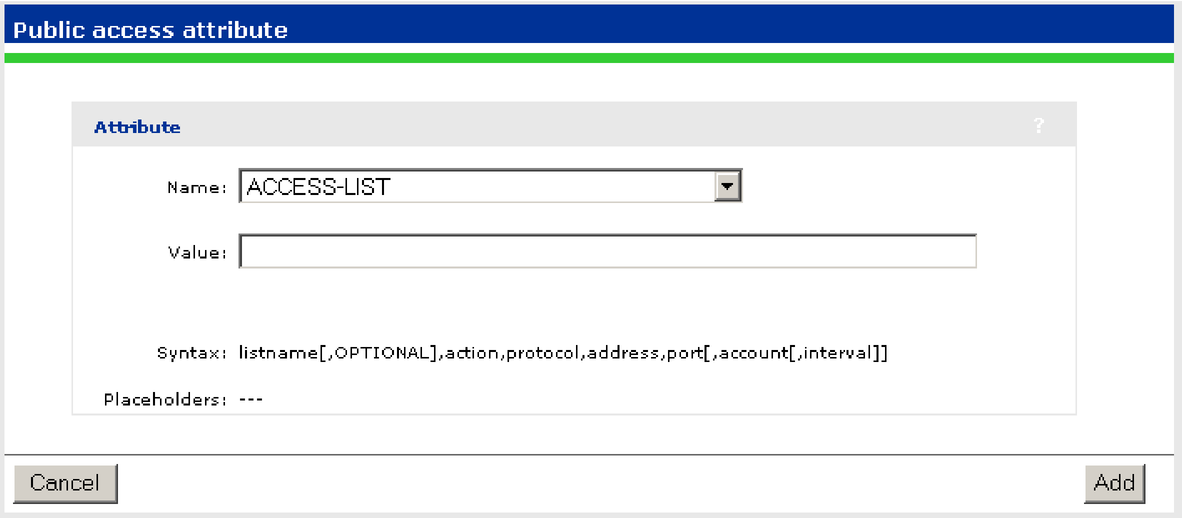
This table lists the currently configured attributes that define settings for the public access interface and user accounts.

This enables you to run the service controller without setting up a RADIUS server to store this configuration information, which is convenient for experimenting with the service controller feature set before deploying it.

If you enable the **Retrieve attributes using RADIUS** option, these same attributes can be defined in the RADIUS account for the service controller. When the service controller authenticates itself, it retrieves the attributes. These attributes will overwrite the settings on this page if the **Retrieved attributes override configured attributes** is enabled.

To add a new attribute:

1 Select **Add New Attribute.** The **Public access attribute** page opens.



Name: ACCESS-LIST

Value:

Syntax: listname[,OPTIONAL],action,protocol,address,port[,account[,interval]]

Placeholders: ---

Figure 11-4: Public Access Attribute

2 Under **Name,** select a type of local configuration attribute, as shown in the following figure.

3 Once you select a **Name,** information appears regarding the correct syntax to specify under **Value.** Use the correct syntax to specify the desired **Value.** For information see the *Network Access Admin Guide*.

4 Select **Add.**

12

Chapter 12 - Local Mesh

In This Chapter:

12.1 Introduction

NOTE

In previous firmware releases, *local mesh* was known as *DWDS* (dynamic wireless distribution system).

NOTE

Local mesh support is available for both controlled and autonomous APs.

The local mesh feature replaces the need for Ethernet cabling between APs, enabling expanded Wi-Fi coverage through the use of wireless bridges to transport network traffic in hard-to-wire or outdoor areas.

Key local mesh features include:

- **Automatic link establishment:** Nodes automatically establish wireless links to create a full-connected network. A dynamic network identifier (local mesh group ID) restricts connectivity to groups of nodes, enabling distinct groups to be created with nodes in the same physical area.

- **Provides fall-back operation to recover from node failure.** In a properly designed implementation, redundant paths can be provided. If a node fails, the mesh will automatically reconfigure itself to maintain connectivity.

12.2 Local Mesh Terminology

The following table defines terms that are used in this guide when discussing the local mesh feature.

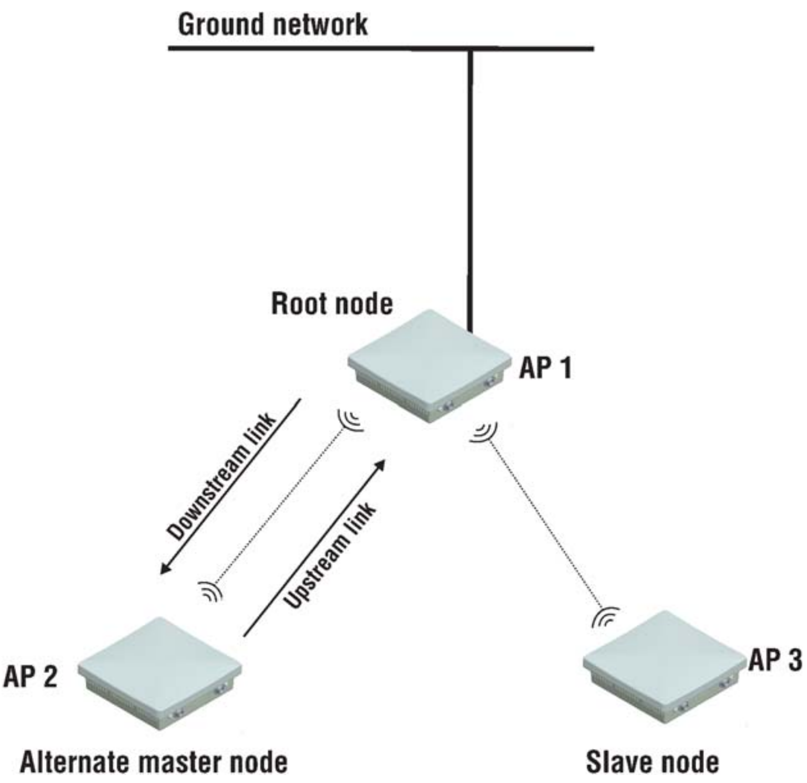


Figure 12-1: Local Mesh Terminology

Term	Definition
Node	A AP that is configured to support local mesh connections.
Root node	The root node is configured in **Master** mode and provides access to the ground network.
Alternate master node	A node that is configured in **Alternate master** mode which enables it to make upstream and downstream connections.
Slave node	A node that is configured in **Slave** mode which enables it to make upstream connections only.
Ground network	Wired network to which the root node is connected. This is the network to which the local mesh provides access for all connected alternate master and slave nodes.

Term	Definition
Mesh	A series of nodes that connect to form a network. Each mesh is identified by a unique mesh ID.
Link	The wireless connection between two nodes.
Downstream link	A link that transports data away from the ground network.
Upstream link	A link that transports data towards the ground network.
Peer	Any two connected nodes are peers. In the diagram, *AP 1* is *the peer of both AP 2 and AP 3.*

12.3 Local Mesh Operational Modes

Three different roles can be assigned to a local mesh node: **Master, Alternate Master,** or **Slave.** Each role governs how upstream and downstream links are established by the node.

- **Master**: Root node that provides the upstream link to the *ground network* that the other nodes want to reach. The master never tries to connect to any other node. It waits for links from downstream alternate master or slave nodes.

NOTE

It is possible to have several masters for the same mesh ID connected to the ground network. This can be used to provide redundant paths to the ground network for downstream nodes.

- **Alternate Master**: First establishes an upstream link with a master or alternate master node. Next, operates as a master node waits for links from downstream alternate master or slave nodes.

- **Slave**: Can only establish an upstream link with master or alternate master node. Slave nodes cannot establish downstream links with other nodes.

12.4 Node Discovery

Discovery of another node to link with is limited to nodes with the same mesh ID. The link is established with the node that has the best score based on the following calculation:

```
  Score = SNR - (Number of hops x SNR cost of each hop)
```

If a node looses its upstream link, it automatically discovers and connects to another available node.

12.5 Operating Channel

If a mesh operates on a dynamic frequency selection (DFS) channel, the master node selects the operating channel. If another node detects radar and switches channels, that node reports the channel switch to the master node, which initiates a channel switch for the nodes connected to it. This allows the local mesh to converge on a specific channel.

A node that uses a DFS channel and that loses connection with its master, scans channels to find a master on another channel, which can be a new master or the same master.

If the local mesh does not operate on a DFS channel, configure the radios in one of the following ways:

- Configure the radios on all nodes to use the same fixed channel.
- Configure the radios for automatic channel selection. In this case the master selects the least noisy channel. Slaves and alternate masters scan channels until they find the master, then tune to the master’s channel and link with the master.

12.6 Local Mesh Profiles

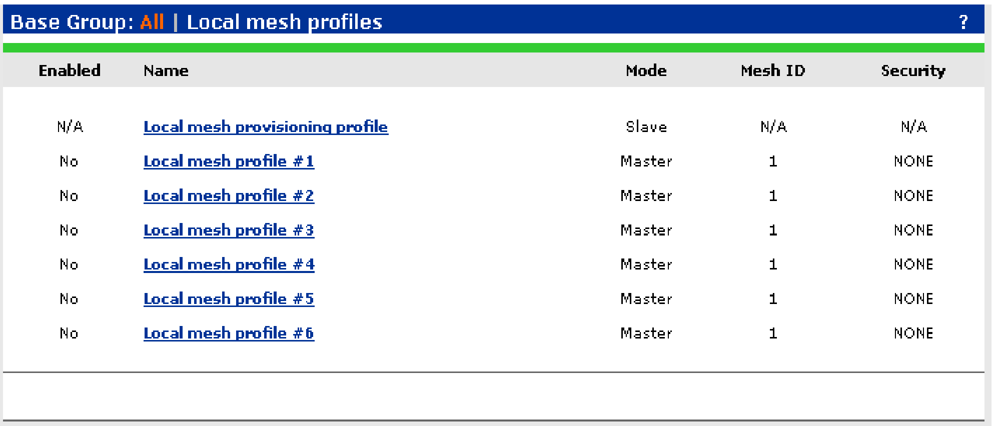
A local mesh profile defines the characteristics for the type of links that can be established with other nodes as follows:

Role	Upstream link	Downstream link
Master	None.	Up to nine links with alternate master or slave nodes.
Alternate master	A single link to a master node or alternate master node.	Up to eight links with alternate master or slave nodes.
Slave	A single link to a master node or alternate master node.	None.

Each node supports up to six profiles plus one provisioning profile. When a profile is active, a node constantly scans and tries to establish links as defined by the profile.

The **local mesh provisioning profile** is used by the wireless link created on a provisioned AP to support discovery of the service controller. Initially, this link operates in slave mode. If you configure this profile as an alternate master, then it can also be used to establish up to nine downstream links with alternate master or slave nodes. See “Provisioning Local Mesh Links” on page 306 for more information.

Local mesh profiles are configurable at either the group or AP level. To view all profiles select **Configuration > Local mesh** for a group or device. The following example shows the local mesh page for the base group.



Base Group: All | Local mesh profiles ?

Enabled	Name	Mode	Mesh ID	Security
N/A	Local mesh provisioning profile	Slave	N/A	N/A
No	Local mesh profile #1	Master	1	NONE
No	Local mesh profile #2	Master	1	NONE
No	Local mesh profile #3	Master	1	NONE
No	Local mesh profile #4	Master	1	NONE
No	Local mesh profile #5	Master	1	NONE
No	Local mesh profile #6	Master	1	NONE

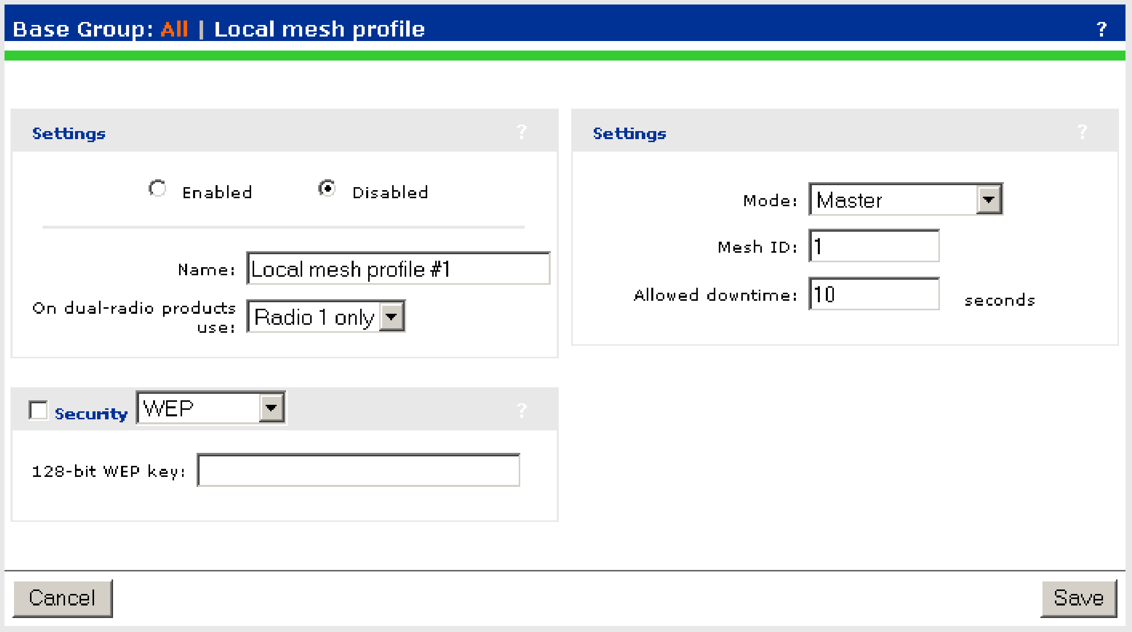
Figure 12-2: Local Mesh Profiles

12.6.1 Configuration Guidelines

- In addition to the provisioning profile, you can configure a total of six local mesh profiles on each node.
- Each local mesh profile (on a master or alternate master) can be used to establish up to nine links with other nodes.
- The same security settings must be used on all nodes in the same mesh.
- Any node that reaches the service controller through the local mesh and uses local mesh itself, must be provisioned prior to discovery.
- Daisy-chaining of nodes using local mesh links reduces throughput (which is typically divided by two for each hop) especially when one or more of the following are true:
  - Nodes provide both upstream and downstream links on the same radio.
  - Nodes share a radio with AP functionality.
  - IP traffic originating from a node can be sent on the link on which the service controller was discovered.

12.6.2 Configuring a Standard Profile

To configure profiles #1 to #6, select a name in the list. The **Local mesh profile** page opens.



Base Group: All | Local mesh profile

Settings

○ Enabled ● Disabled

Name: Local mesh profile #1

On dual-radio products use: Radio 1 only

Settings

Mode: Master

Mesh ID: 1

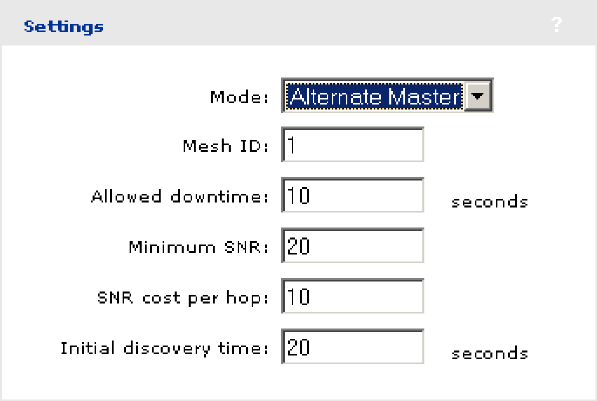
Allowed downtime: 10 seconds

□ Security WEP

128-bit WEP key:

Figure 12-3: Configuring a Standard Profile

For **Slave** and **Alternate Master**, the **Settings** box shows the following additional options:



Settings

Mode: Alternate Master

Mesh ID: 1

Allowed downtime: 10 seconds

Minimum SNR: 20

SNR cost per hop: 10

Initial discovery time: 20 seconds

Figure 12-4:

12.6.2.1 General

12.6.2.1.1 Enabled/Disabled

Specify if the profile is enabled or disabled. The profile is only active when enabled.

12.6.2.1.2 Name

Name of the profile.

12.6.2.2 Settings

12.6.2.2.1 Mode

Three different roles can be assigned to a node: master, alternate master, or slave. Each role governs how links are established. Links are defined as either upstream or downstream.

- **Master:** The master is the root node that provides the upstream connection to the *ground network* that the other nodes want to reach. The master will only create downstream local mesh links to alternate master or slave nodes.

- **Slave:** Slave nodes can only establish upstream links with master or alternate master nodes. Slave nodes cannot establish downstream links with other nodes.

- **Alternate Master:** An alternate master node must first establish an upstream link with a master or alternate master node before it can establish downstream connections with an alternate master or slave node.

12.6.2.2.2 Mesh ID

Unique number that identifies a series of nodes that can connect together to form a local mesh network.

12.6.2.2.3 Allowed Downtime

The maximum time (in seconds) that a link can remain idle before the link actually gets deleted. When a slave (or alternate master) looses its link to its master, the discovery phase is re-initiated.

12.6.2.2.4 Minimum SNR

(Alternate master or slave nodes)

This node will only connect with other nodes whose SNR is above this setting (in dB).

12.6.2.2.5 SNR Cost Per Hop

(Alternate master or slave nodes)

This value is an estimate of the cost of a hop in terms of SNR. It indicates how much SNR a node is willing to sacrifice to connect to node one hop closer to the root node, because each hop has an impact on performance, especially when using a single radio.

12.6.2.2.6 Initial Discovery Time

(Alternate master or slave nodes)

Amount of time that will be taken to discover the best available master node. The goal of this setting is to delay discovery until all the nodes in the surrounding area have had time to startup, making the identification of the best master more accurate. If this period is too short, a slave may connect to the first master it finds, not necessarily the best.

12.6.2.3 Security

Enable this option to secure data transmitted on the wireless link. The APs on both sides of the wireless link must be configured with the same security options.

12.6.2.3.1 WEP

Enables WEP to secure traffic on the wireless link.

Specify the encryption key the node will use to encrypt/decrypt all data it sends and receives. The key is 128 bits long and must be specified as 26 hexadecimal digits.

12.6.2.3.2 TKIP

Enables TKIP encryption to secure traffic on the wireless link.

The node uses the key you specify in the PSK field to generate the TKIP keys that encrypt the wireless data stream.

Specify a key that is between 8 and 64 ASCII characters in length. It is recommended that the key be at least 20 characters long, and be a mix of letters and numbers.

12.6.2.3.3 AES/CCMP

Enables AES with CCMP encryption to secure traffic on the wireless link. This is the most secure method.

The node uses the key you specify in the PSK field to generate the keys that encrypt the wireless data stream.

Specify a key that is between 8 and 64 ASCII characters in length. It is recommended that the key be at least 20 characters long and be a mix of letters and numbers.

12.6.3 Other Configuration Settings

12.6.3.1 Simultaneous AP and Local Mesh

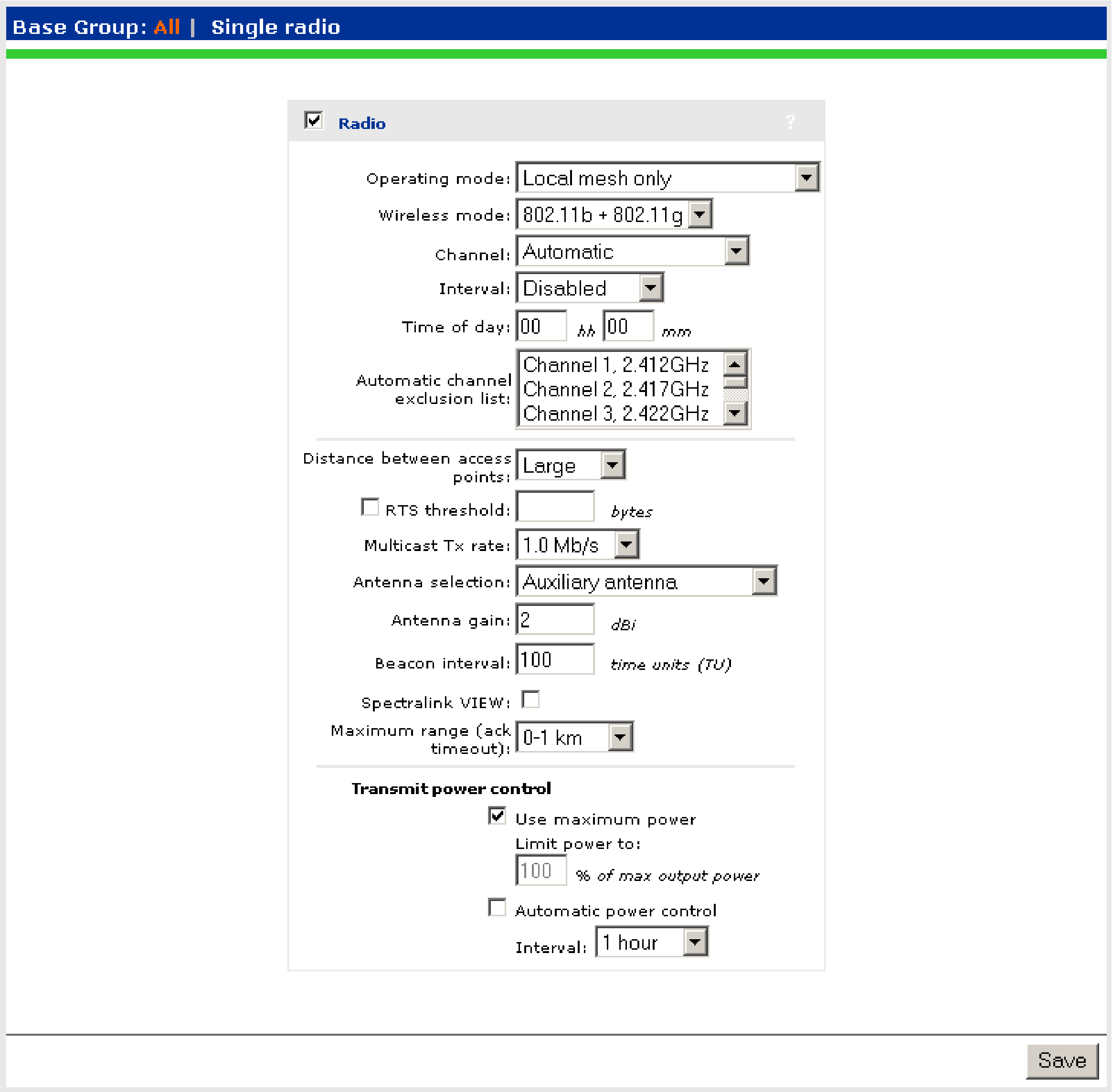
A radio can be configured to simultaneously support wireless clients and the creation of one or more local meshes. Although this offers flexibility it does have several limitations as follows:

- It reduces overall throughput since the total available bandwidth is shared between the local meshes and wireless users.
- It limits you to using the same radio options for both wireless clients and local meshes.

12.6.3.2 Maximum Range (Ack Timeout)

This is a global setting that is configurable on the **Radio** page when the **Operating mode** is set to **Local mesh**. It fine tunes internal timeout settings to account for the distance that a link spans. For normal operation, it is set to less than 1 km.

This is a global setting that applies to all wireless connections made with a radio, not just for local mesh links. Therefore, if you are also using a radio to as an AP, adjusting this setting may lower the performance for users with marginal signal strength or when interference is present. (Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)



Base Group: All | Single radio

☑ Radio

Operating mode: Local mesh only

Wireless mode: 802.11b + 802.11g

Channel: Automatic

Interval: Disabled

Time of day: 00 *hh* 00 *mm*

Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz

Distance between access points: Large

□ RTS threshold: *bytes*

Multicast Tx rate: 1.0 Mb/s

Antenna selection: Auxiliary antenna

Antenna gain: 2 *dBi*

Beacon interval: 100 *time units (TU)*

Spectralink VIEW: □

Maximum range (ack timeout): 0-1 km

Transmit power control

☑ Use maximum power

Limit power to:

100 *% of max output power*

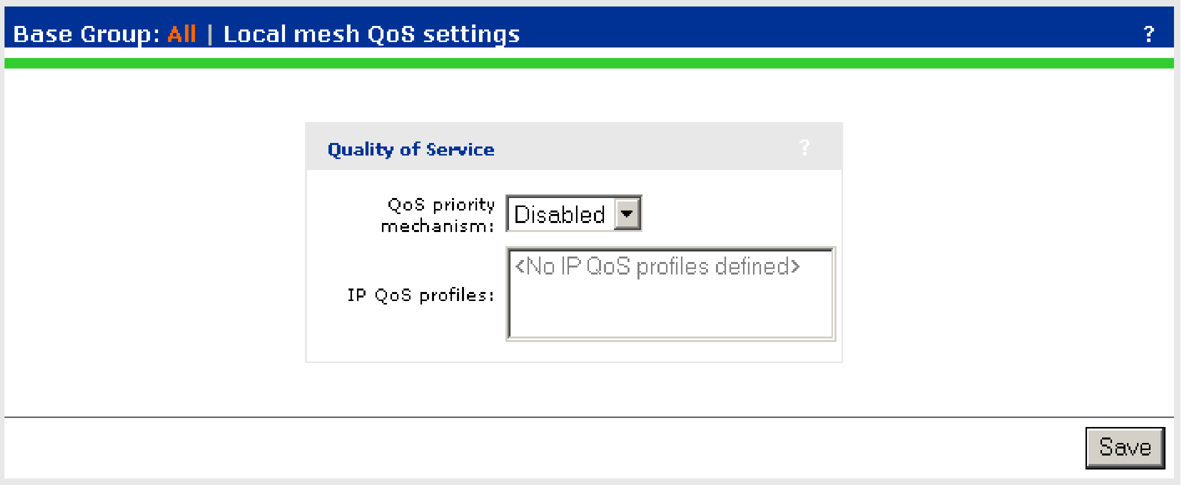
□ Automatic power control

Interval: 1 hour

Figure 12-5: Single Radio

12.6.3.3 Quality of Service

The local mesh feature enables you to define a quality of service (QoS) setting that will govern how traffic is sent on all wireless links.



Base Group: All | Local mesh QoS settings

Quality of Service

QoS priority mechanism: Disabled

IP QoS profiles: <No IP QoS profiles defined>

Figure 12-6: Local Mesh QoS Settings

The QoS setting on all nodes in a local mesh must be the same.

NOTE

When traffic is forwarded onto a local mesh link from a virtual network, the QoS settings on the virtual network take priority. For example, if you define a virtual network with a QoS setting of virtual network-based High, then traffic from this virtual network will traverse the bridge on queue 2 even if the QoS setting on the bridge is virtual network-based Low (queue 4).

12.7 Provisioning Local Mesh Links

APs operating in controlled mode must be able to discover and connect with a service controller. When operating as part of a local mesh, *any AP that can only discover the service controller via a wireless link must be provisioned* before being deployed. In this example, AP 1, AP 2, and AP 4 must be provisioned prior to deployment for discovery to be successful.

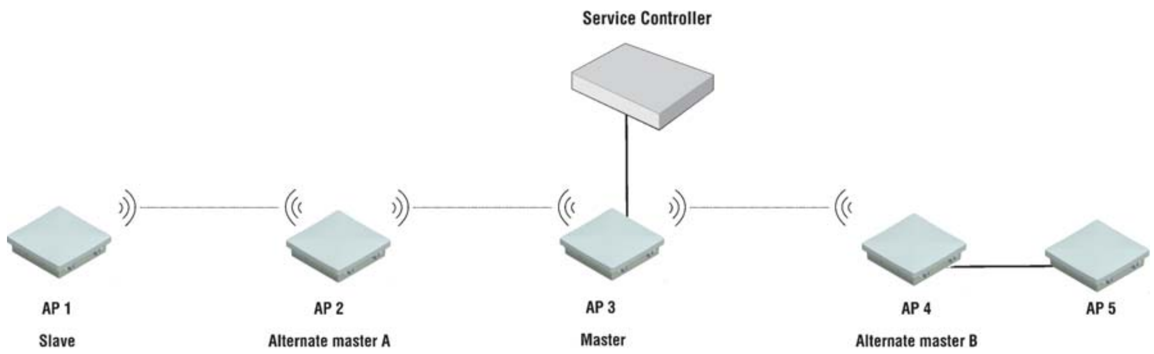


Figure 12-7: Provisioning Local Mesh Links

Provisioning is done before APs are deployed using either of the following methods:

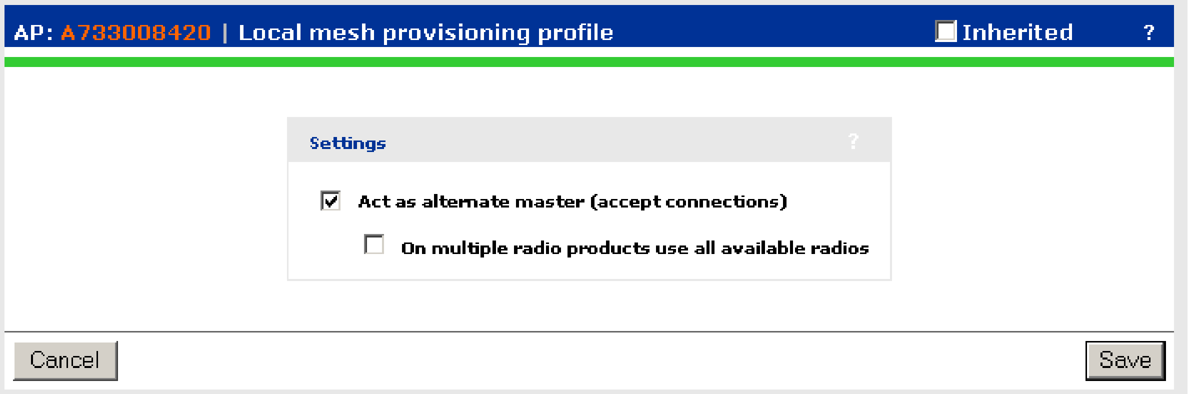
- Directly connect to each AP and use its management tool to define provisioning settings.
- Connect the APs to the service controller (either directly via the LAN port or through a local area network). After the APs are discovered, use the service controller's management tool to define provisioning settings by opening the **Provisioning** > **Connectivity** page at either the group or AP level.

NOTE

The service controller and all APs must all be configured for the same country, so that the local mesh established respects your local RF regulations. The service controller country setting is defined by selecting **Service Controller >> Management > Country**. APs with the wrong country setting will be displayed with a diagnostic of **Invalid Country** on the **Controlled APs >> Overview** page.

The local mesh provisioning profile for AP 1 needs to be set to alternate master mode so that it can support a connection from AP 2. Select AP 1 in the **Network**

Tree and then open the **Configuration > Local mesh** page and select **Local mesh provisioning profile.**



AP: A733008420 | Local mesh provisioning profile

☐ Inherited

Settings

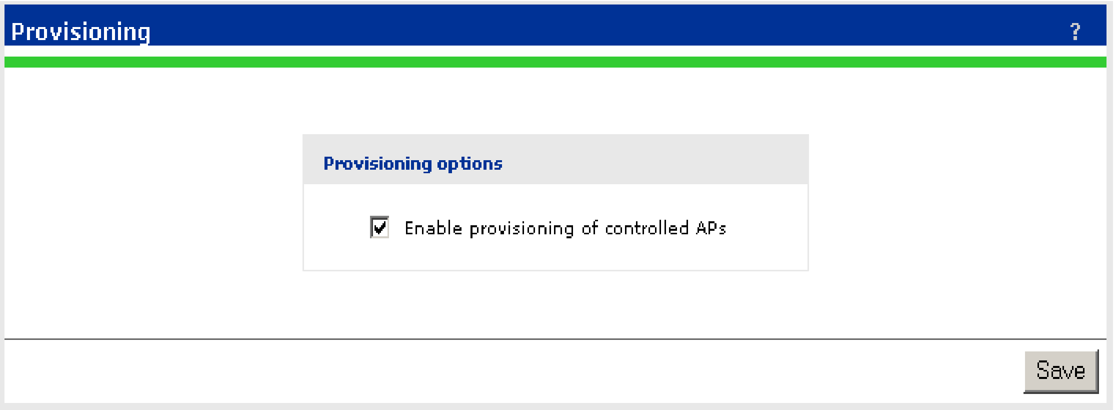
☑ Act as alternate master (accept connections)

☐ On multiple radio products use all available radios

Figure 12-8: Local Mesh Provisioning Profile

NOTE

To enable the service controller to send provisioned settings to controlled APs, by activating the **Enable provisioning of controlled APs** option on the **Service Controller >> Controlled APs > Provisioning** page.



Provisioning

Provisioning options

☑ Enable provisioning of controlled APs

Figure 12-9: Provisioning

Until this option is enabled, provisioned settings defined on the service controller are not sent to any controlled APs.

Once provisioning settings have been defined you need to update all controlled APs with the new settings by synchronizing them as described in "Synchronizing APs" on page 65.

After an AP has been updated with provisioned settings, the provisioned settings do not become active until the AP is restarted, or a **Remove and rediscover** action is executed on the **Controlled APs >> Configured APs** page.

12.8 How to Configure Local Mesh in Controlled Mode

The configuration of local mesh in controlled mode comprises the following steps:

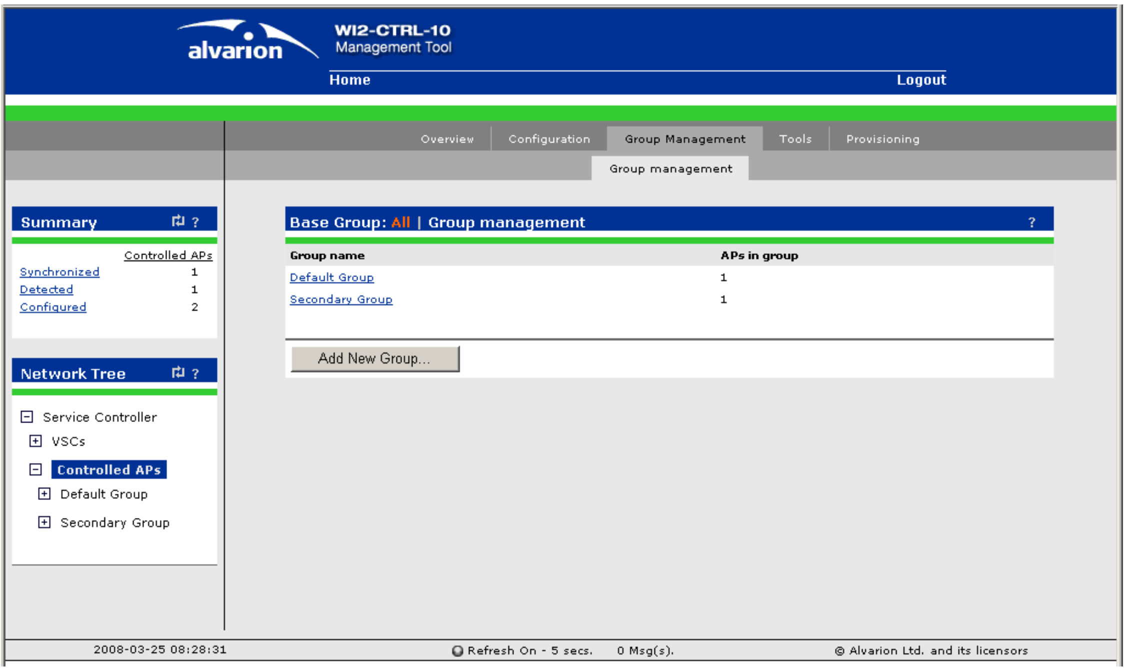
- Setting a Master Profile
- Setting the Master AP
- Setting the SLAVE AP
- Adding the Slave AP in a Group on the Controller

12.8.1 Setting a Master Profile

To set a Master Profile:

Using a factory reset controller do the following:

1. Creat a new Group within the controller by clicking on "**Controlled APs** > **Group Management** > **Add a new group**"



Summary

	Controlled APs
Synchronized	1
Detected	1
Configured	2

Network Tree

- Service Controller
  - VSCs
  - Controlled APs
    - Default Group
    - Secondary Group

Base Group: All | Group management

Group name	APs in group
Default Group	1
Secondary Group	1

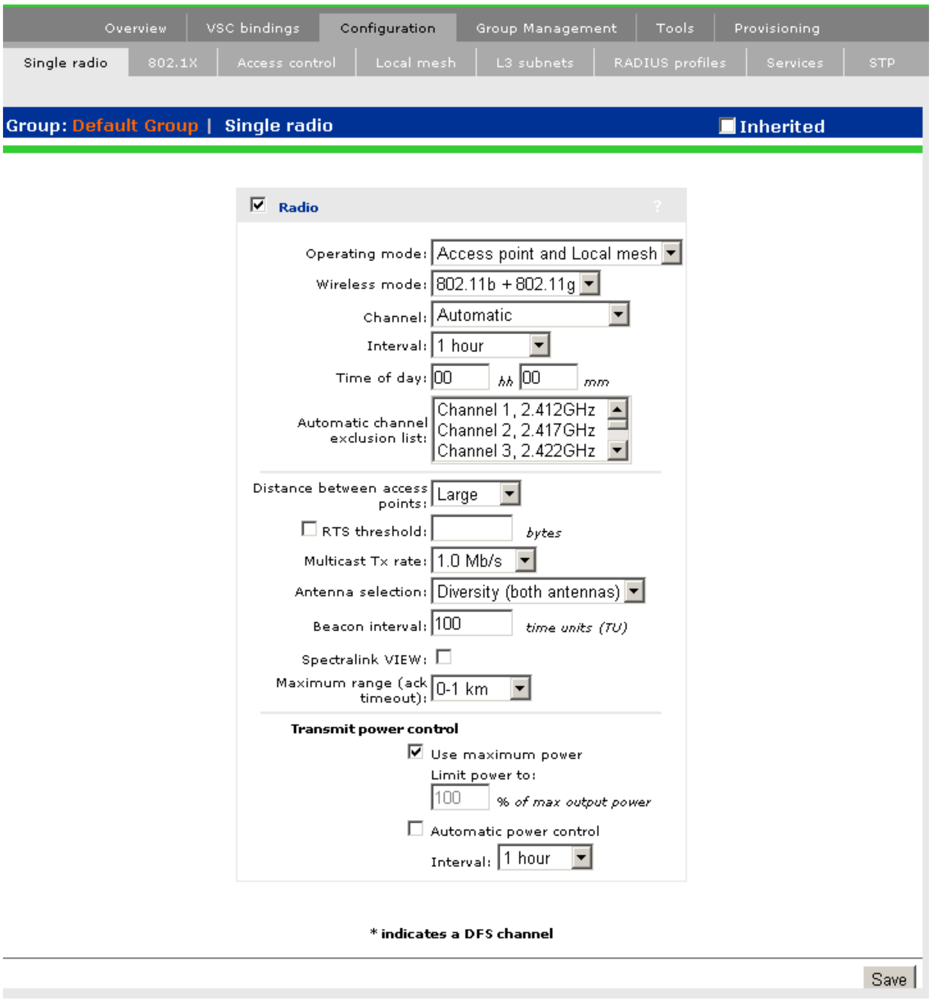
2008-03-25 08:28:31 Refresh On - 5 secs. 0 Msg(s). © Alvarion Ltd. and its licensors

Figure 12-10: Group Management

2 Access the created group and click on the "Configuration" tab. The "Single Radio" page is displayed.

a Uncheck the "Inherited" check box

b Configure the Radio page as follows:



Group: Default Group | Single radio ☐ Inherited

☑ Radio

Operating mode: Access point and Local mesh

Wireless mode: 802.11b + 802.11g

Channel: Automatic

Interval: 1 hour

Time of day: 00 *hh* 00 *mm*

Automatic channel exclusion list: Channel 1, 2.412GHz
Channel 2, 2.417GHz
Channel 3, 2.422GHz

Distance between access points: Large

☐ RTS threshold: *bytes*

Multicast Tx rate: 1.0 Mb/s

Antenna selection: Diversity (both antennas)

Beacon interval: 100 *time units (TU)*

Spectralink VIEW: ☐

Maximum range (ack timeout): 0-1 km

Transmit power control

☑ Use maximum power

Limit power to:

100 *% of max output power*

☐ Automatic power control

Interval: 1 hour

*** indicates a DFS channel**

Figure 12-11: Single Radio Page

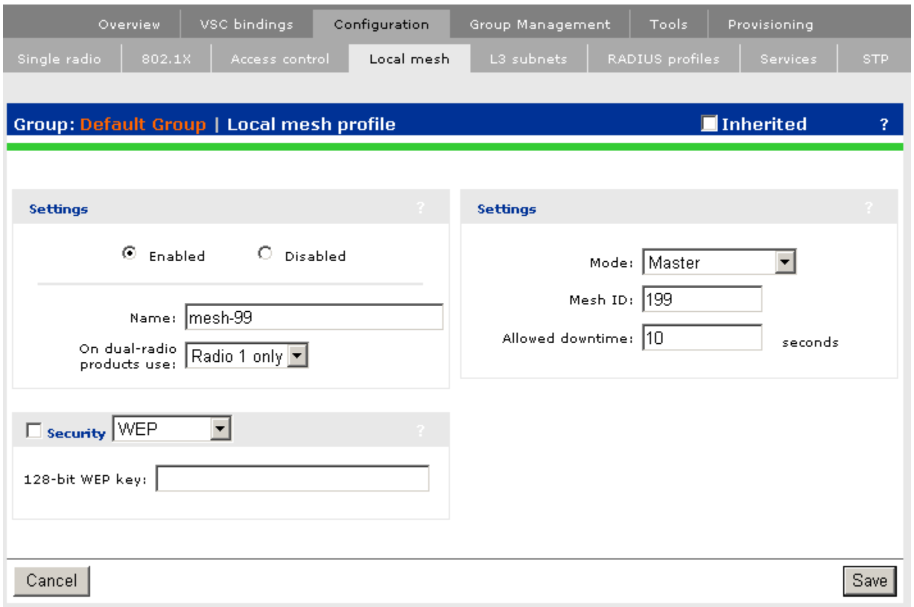
c Save your changes

4 Click on the "Local Mesh" tab located also under "Configuration"

a Select "Local Mesh Profile # 1"

b Uncheck the "Inherited" check box

c Configure the profile as follows:



Group: Default Group | Local mesh profile ☐ Inherited

Settings

● Enabled ○ Disabled

Name: mesh-99

On dual-radio products use: Radio 1 only

☐ Security WEP

128-bit WEP key:

Settings

Mode: Master

Mesh ID: 199

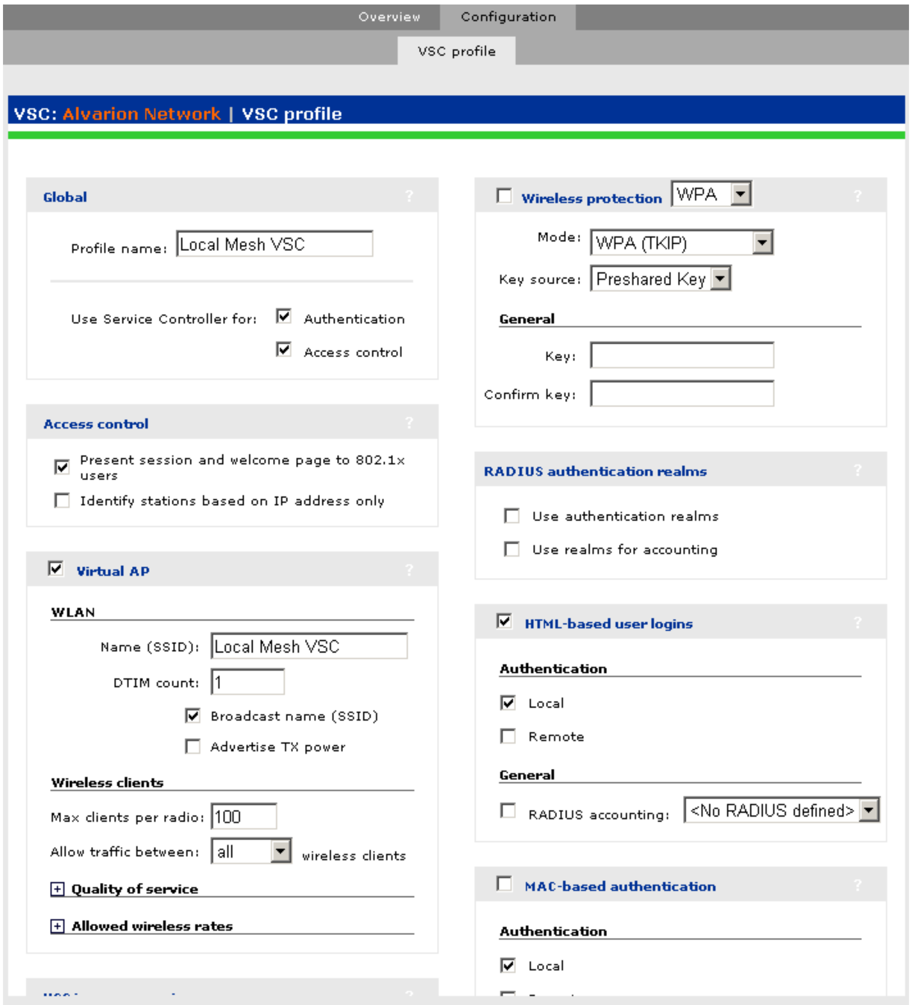
Allowed downtime: 10 seconds

Figure 12-12: Local Mesh Profile

d Save your configuration

5 Click on the "VSC" link in the Navigation tree bar

a Reconfigure the default VSC OR Click on the "Add a new VSC" Button, and configure a VSC as follows:



VSC: Alvarion Network | VSC profile

Global

Profile name: Local Mesh VSC

Use Service Controller for: ☑ Authentication ☑ Access control

Access control

☑ Present session and welcome page to 802.1x users

□ Identify stations based on IP address only

☑ **Virtual AP**

WLAN

Name (SSID): Local Mesh VSC

DTIM count: 1

☑ Broadcast name (SSID)

□ Advertise TX power

Wireless clients

Max clients per radio: 100

Allow traffic between: all wireless clients

⊞ Quality of service

⊞ Allowed wireless rates

□ **Wireless protection** WPA

Mode: WPA (TKIP)

Key source: Preshared Key

General

Key:

Confirm key:

RADIUS authentication realms

□ Use authentication realms

□ Use realms for accounting

☑ **HTML-based user logins**

Authentication

☑ Local

□ Remote

General

□ RADIUS accounting: <No RADIUS defined>

□ **MAC-based authentication**

Authentication

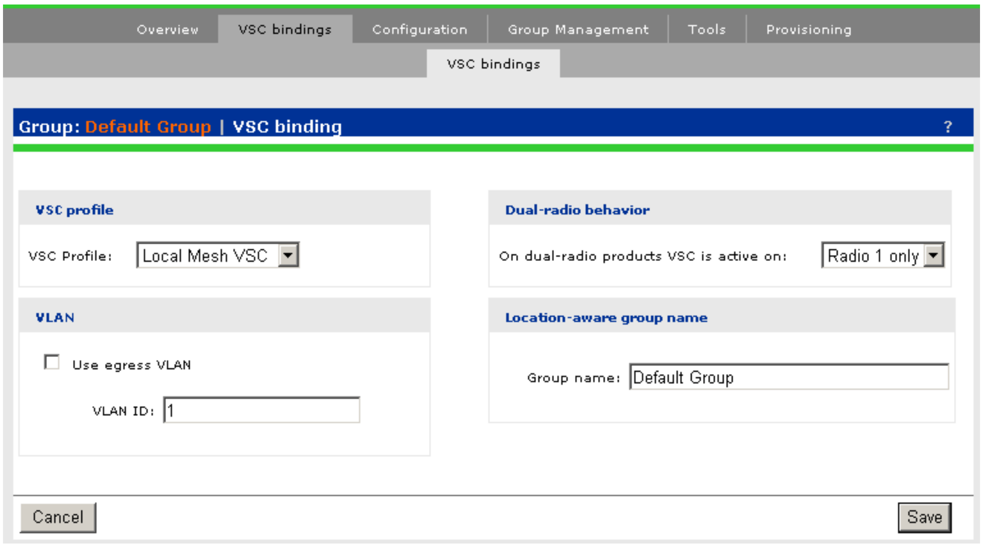
☑ Local

Figure 12-13: VSC Profile

- **b** Save your configuration

3 Access the Group created in Section 12.8.1 step1 above and click on the "VSC Bindings" tab.

- **a** Click on the "Add New Binding" button
- **b** Select the created VSC name in the "VSC Profile" menu as follows:



Group: Default Group | VSC binding

VSC profile

VSC Profile: Local Mesh VSC

Dual-radio behavior

On dual-radio products VSC is active on: Radio 1 only

VLAN

□ Use egress VLAN

VLAN ID: 1

Location-aware group name

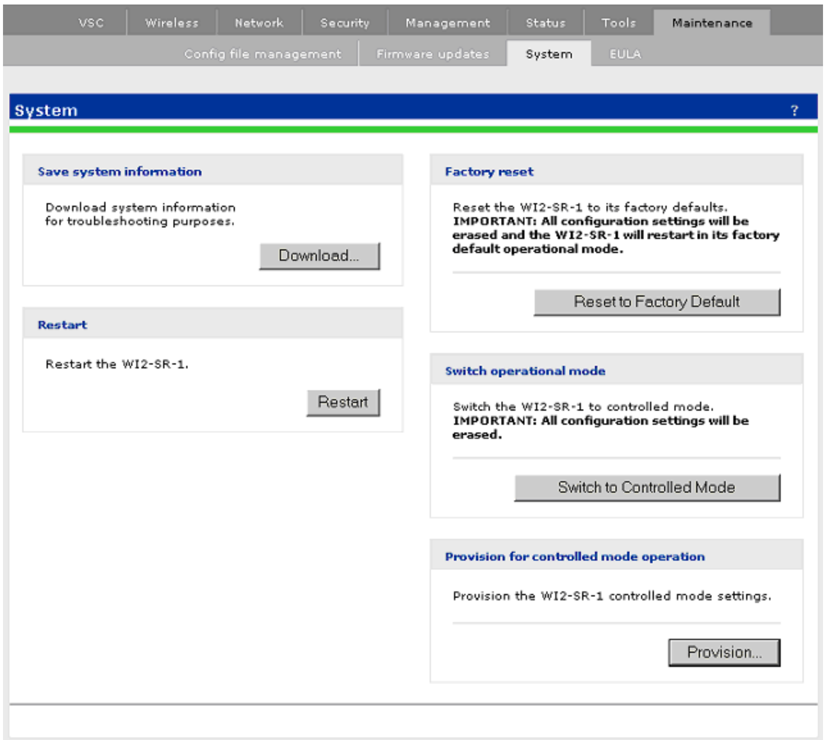
Group name: Default Group

Figure 12-14: VSC Bindings

c Save your configuration

12.8.2 Setting the Master AP

1. Power UP an AP in Autonomous mode (Alvarion Default Mode)
2. Login to the AP's web tool
3. Click on "Maintenance > System"
4. Click on the "Switch to Controlled Mode" button to switch the MASTER AP into Controlled mode as shown below:



System

Save system information

Download system information for troubleshooting purposes.

Restart

Restart the WI2-SR-1.

Factory reset

Reset the WI2-SR-1 to its factory defaults. **IMPORTANT: All configuration settings will be erased and the WI2-SR-1 will restart in its factory default operational mode.**

Switch operational mode

Switch the WI2-SR-1 to controlled mode. **IMPORTANT: All configuration settings will be erased.**

Provision for controlled mode operation

Provision the WI2-SR-1 controlled mode settings.

Figure 12-15: Switch to Controlled Mode

5 When this AP is back UP, place it on the same subnet as your controller

6 The AP should now discover the controller and synchs UP in the controller's DEFAULT GROUP

7 Drag and drop this AP from the DEFAULT GROUP into the created group in Section 12.8.1 step1

8 The AP should now synch into the created group restoring all the configuration done in STEPS (2 - 5)

9 Now you will have an active VSC bounded to the MASTER

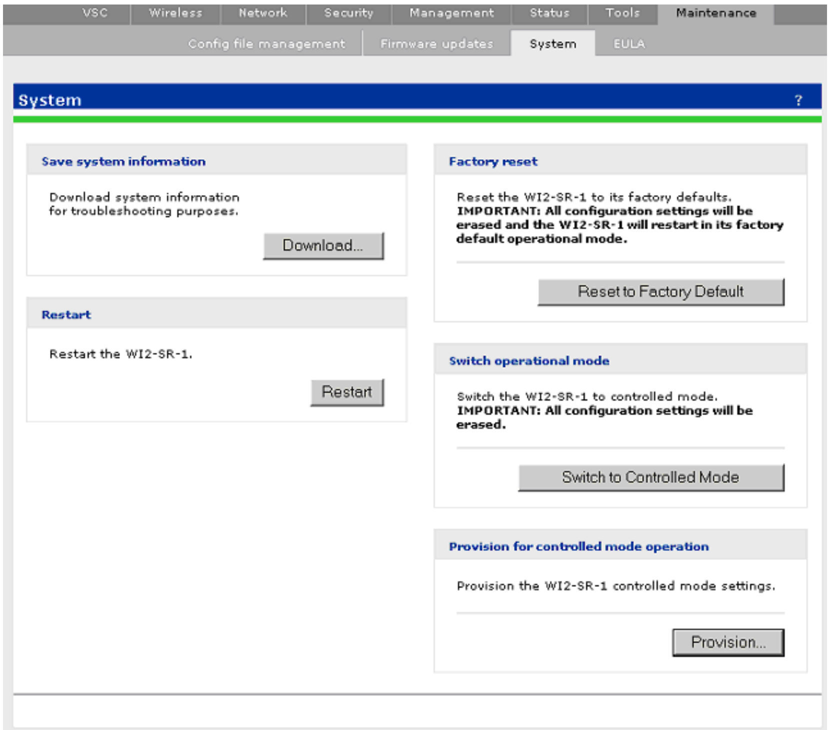
12.8.3 Setting the SLAVE AP

1 Power UP another AP in Autonomous mode (Alvarion Default Mode)

2 Login to the AP's web tool

3 Click on "Maintenance > System"

4 Click on the "Provisioning" button at the bottom on this page to start provisioning the SLAVE AP



System

Save system information

Download system information for troubleshooting purposes.

Restart

Restart the WI2-SR-1.

Factory reset

Reset the WI2-SR-1 to its factory defaults. **IMPORTANT: All configuration settings will be erased and the WI2-SR-1 will restart in its factory default operational mode.**

Switch operational mode

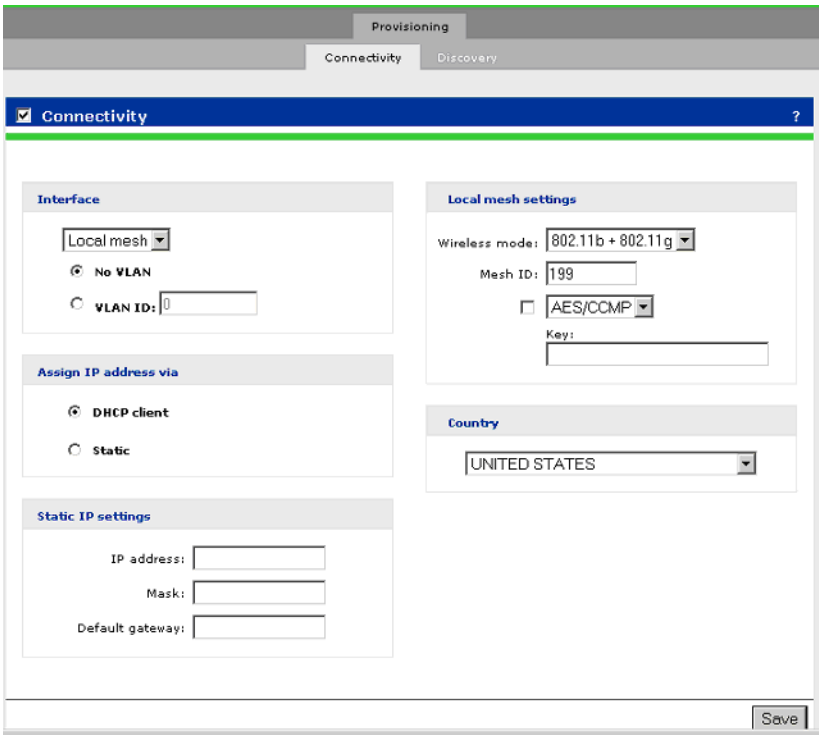
Switch the WI2-SR-1 to controlled mode. **IMPORTANT: All configuration settings will be erased.**

Provision for controlled mode operation

Provision the WI2-SR-1 controlled mode settings.

Figure 12-16: Provisioning the Slave AP

5 Starting with the "Connectivity" sub-page, configure as follows:



☑ Connectivity

Interface

Local mesh

● No VLAN

○ VLAN ID: 0

Assign IP address via

● DHCP client

○ Static

Static IP settings

IP address:

Mask:

Default gateway:

Local mesh settings

Wireless mode: 802.11b + 802.11g

Mesh ID: 199

□ AES/CCMP

Key:

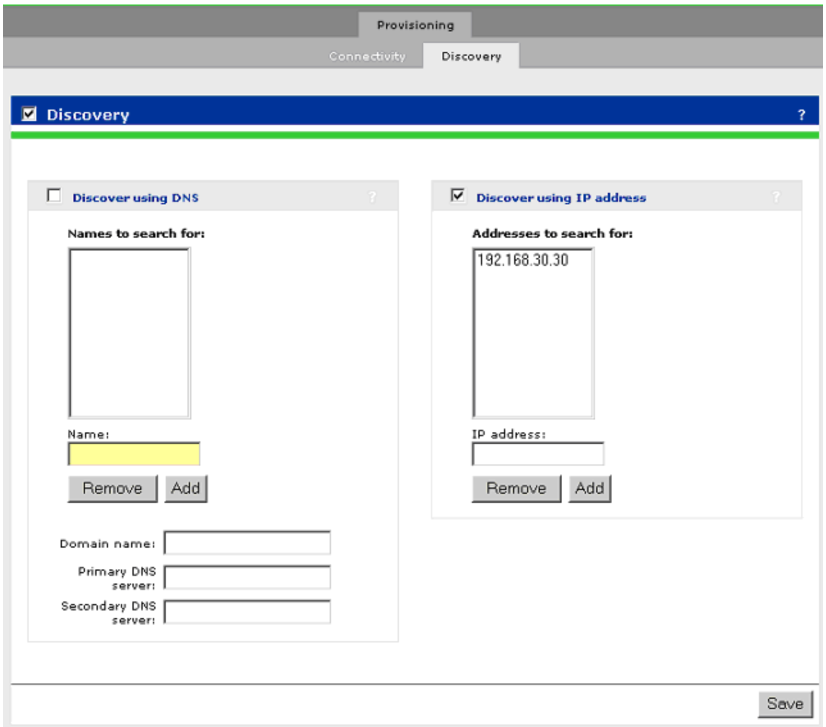
Country

UNITED STATES

Figure 12-17: Connectivity Page

6 Save your configuration

7 Click on the Discovery sub-tab (within the provisioning page), and configure as follows:



☑ Discovery

□ Discover using DNS

Names to search for:

Name:

Domain name:

Primary DNS server:

Secondary DNS server:

☑ Discover using IP address

Addresses to search for:

192.168.30.30

IP address:

Figure 12-18: Discovery Page

NOTE

That the IP address showing in the "Discover using IP address" list should be your controller IP address

8 Save your Configuration.

9 Restart the AP by clicking on the restart button on this page.

12.8.4 Adding the Slave AP in a Group on the Controller

1 The provisioned SLAVE AP should discover the Controller over the Mesh Link. (Leave the SLAVE AP in the DEFAULT GROUP for now.)

NOTE

The Master and Slave APs can either share a group or be placed in different Groups. This section shows the different groups path for simplicity.

2 Creat a new Group within the controller by clicking on "Controlled APs > Group Management > Add a new group" (see Figure 12-10)

3 Access the created group and click on the "Configuration" tab. The "Single Radio" page is displayed.

a Uncheck the "Inherited" check box

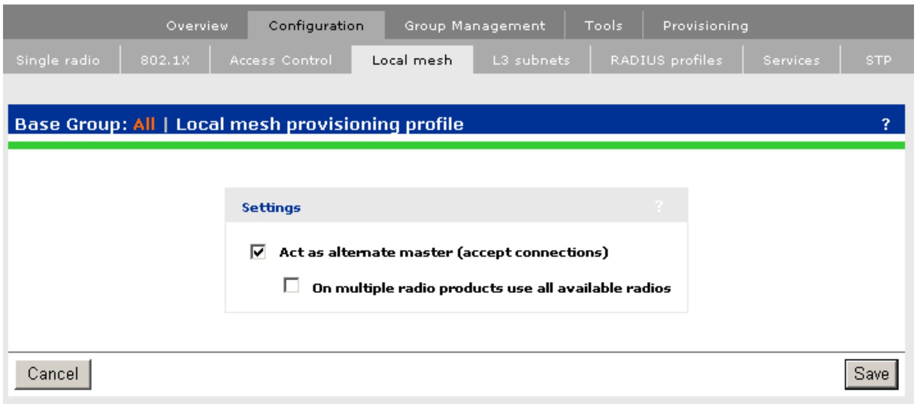
b Configure the Radio page as in Figure 12-11.

c Save your Configuration

4 Click on the "Local Mesh" tab located also under "Configuration"

a Select "Local Mesh Provisioning Profile"

b Configure as follows:



Base Group: All | Local mesh provisioning profile

Settings

☑ Act as alternate master (accept connections)

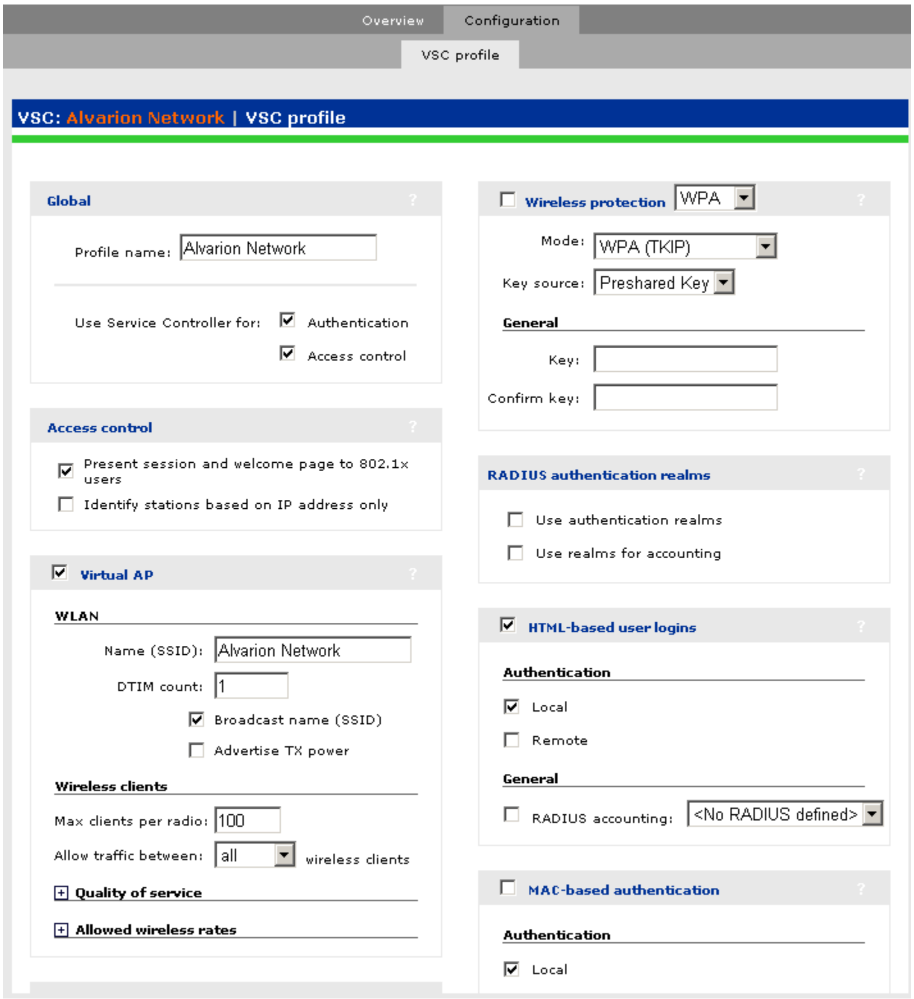
☐ On multiple radio products use all available radios

Figure 12-19: Local Mesh Provisioning Profile

c Save your configuration.

4 Click on the "VSC" link in the Navigation tree bar

a Click on the "Add a new VSC" Button, and configure a VSC as follows (with a different SSID than the Masters):



VSC: Alvarion Network | VSC profile

Global

Profile name: Alvarion Network

Use Service Controller for: ☑ Authentication ☑ Access control

Access control

☑ Present session and welcome page to 802.1x users

□ Identify stations based on IP address only

☑ **Virtual AP**

WLAN

Name (SSID): Alvarion Network

DTIM count: 1

☑ Broadcast name (SSID)

□ Advertise TX power

Wireless clients

Max clients per radio: 100

Allow traffic between: all wireless clients

⊞ **Quality of service**

⊞ **Allowed wireless rates**

□ **Wireless protection** WPA

Mode: WPA (TKIP)

Key source: Preshared Key

General

Key:

Confirm key:

RADIUS authentication realms

□ Use authentication realms

□ Use realms for accounting

☑ **HTML-based user logins**

Authentication

☑ Local

□ Remote

General

□ RADIUS accounting: <No RADIUS defined>

□ **MAC-based authentication**

Authentication

☑ Local

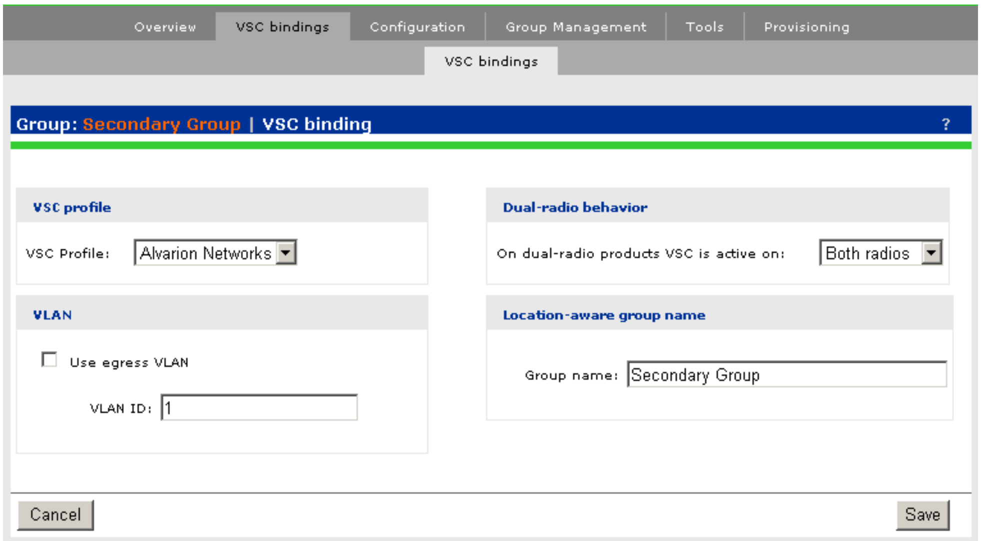
Figure 12-20: Adding a New VSC

b Save your configuration.

3 Access the Group created in Section 12.8.4 step 2 above and click on the "VSC Bindings" tab.

a Click on the "Add New Binding" button

b Select the created SLAVE VSC name in the "VSC Profile" menu as follows:



Group: Secondary Group | VSC binding

VSC profile

VSC Profile: Alvarion Networks

Dual-radio behavior

On dual-radio products VSC is active on: Both radios

VLAN

☐ Use egress VLAN

VLAN ID: 1

Location-aware group name

Group name: Secondary Group

Figure 12-21: VSC Bindings - Slave

c Save your configuration.

4 Drag and drop this AP from the DEFAULT GROUP into the created group in Section 12.8.4 step 1.

5 The AP should now synch into the created group restoring all the configuration done in STEPS (3 - 5)

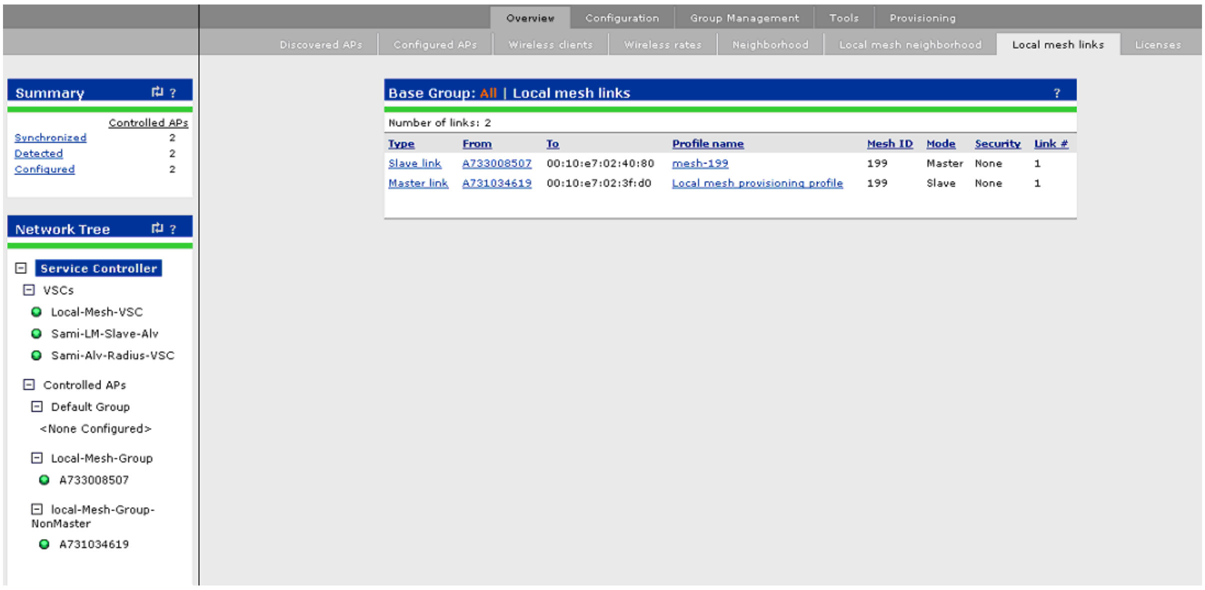
6 You now have an Active VSC on the SLAVE AP and a Local Mesh Link between the MASTER and the SLAVE.

12.8.5 Operation Verification

➤ **To verify that the link is UP:**

1 Click on the "Controlled AP" link on the navigation tree of the Controller.

2 Click on "Local Mesh Link", you should see links that looks like the following:



Summary

	Controlled APs
Synchronized	2
Detected	2
Configured	2

Base Group: All | Local mesh links

Number of links: 2

Type	From	To	Profile name	Mesh ID	Mode	Security	Link #
Slave link	A733008507	00:10:e7:02:40:80	mesh-199	199	Master	None	1
Master link	A731034619	00:10:e7:02:3f:d0	Local mesh provisioning profile	199	Slave	None	1

Figure 12-22: Link Verification

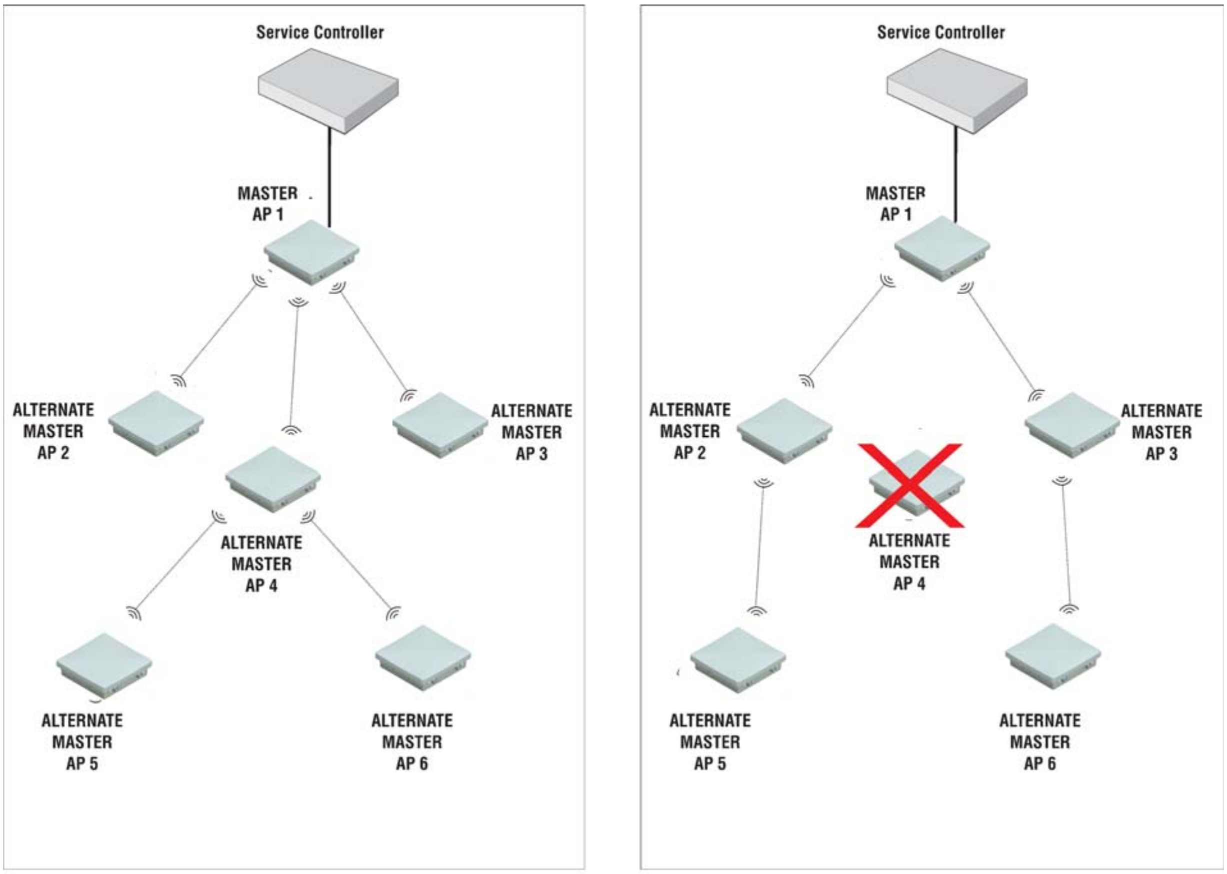
12.9 Sample Local Mesh Deployments

12.9.1 Dynamic Network

In this scenario, a service controller is deployed with several APs to provide wireless coverage of a large area. Instead of using a backbone LAN, wireless links are used to interconnect all APs.

AP 1 is the *master*. It provides the connection to the wired network and a wireless link to the other APs. The other APs automatically established their links to the master based on a balance between SNR (signal to noise ratio) and hops, to provide the most efficient network topology.

If a node becomes unavailable, the links dynamically adjust to find the optimum path to the master.



Initial network configuration is automatically established.

When AP 4 is unavailable, the network dynamically reconfigures itself.

Figure 12-23: Sample Local Mesh Deployment

13

Chapter 13 - Working with Autonomous APs

In This Chapter:

13.1 Key Concepts

This chapter describes how to use the service controller in conjunction with autonomous APs.

TIP

Most of this chapter applies to working with autonomous APs from Alvarion Ltd. For information on working with third-party autonomous APs, see page 9.

APs can operate in either controlled mode or autonomous mode. In controlled mode, the service controller provides centralized management of APs. This is the preferred operation mode. (For more information, see "Working with Controlled APs" on page 37.)

However, in some other cases it is necessary to operate APs in autonomous mode, for example under the following circumstances:

- When an AP is used to create a static WDS (local mesh) link. Controlled mode does not support static local mesh links. It is strongly recommended that dynamic WDS (local mesh) links be used. They provide the same capabilities but with greater flexibility. Furthermore, local mesh is supported in controlled mode.
- A Wi² AP series AP at AOS 4.x or earlier is used. Controlled mode is available on Wi² AP series APs at AOS 5.x or higher. It is strongly recommended that service controllers and APs be upgraded to the same AOS release, and preferably 5.x or higher.

It is recommended that you operate most Wi² AP series APs in controlled mode, reserving autonomous mode only for APs that need features unique to autonomous mode. In autonomous mode, the following functionality is not available: Centralized management, L3 mobility, and WPA2 Opportunistic key caching.

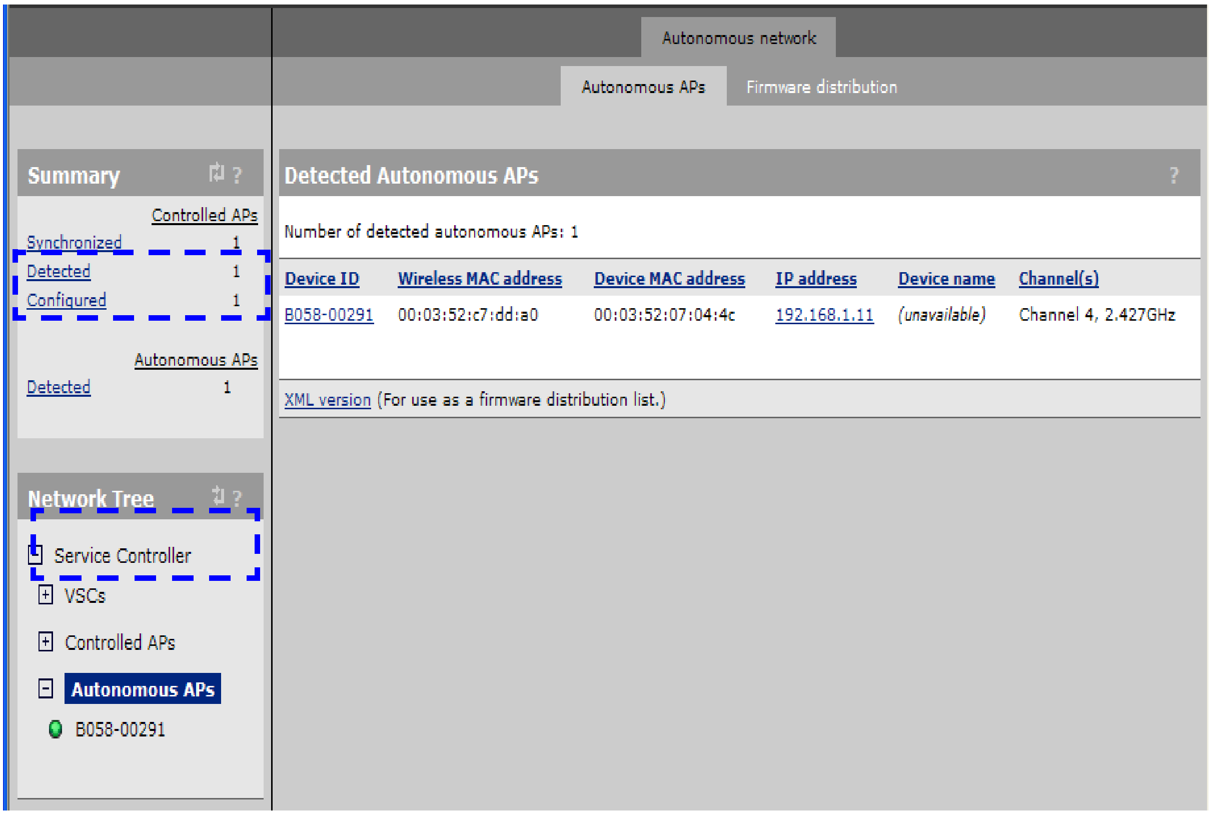
13.1.1 Autonomous AP Detection

The service controller automatically detects all autonomous APs that have their CDP discovery option enabled (default setting) and are installed on the same subnet as the service controller.

To configure this CDP discovery, select **Network > CDP** on the AP's management tool.

13.1.2 Viewing Autonomous AP Information

When the service controller detects at least one autonomous AP, the **Summary** box and the **Network Tree** are updated to include autonomous AP information as follows:



Summary

	Controlled APs
Synchronized	1
Detected	1
Configured	1

	Autonomous APs
Detected	1

Detected Autonomous APs

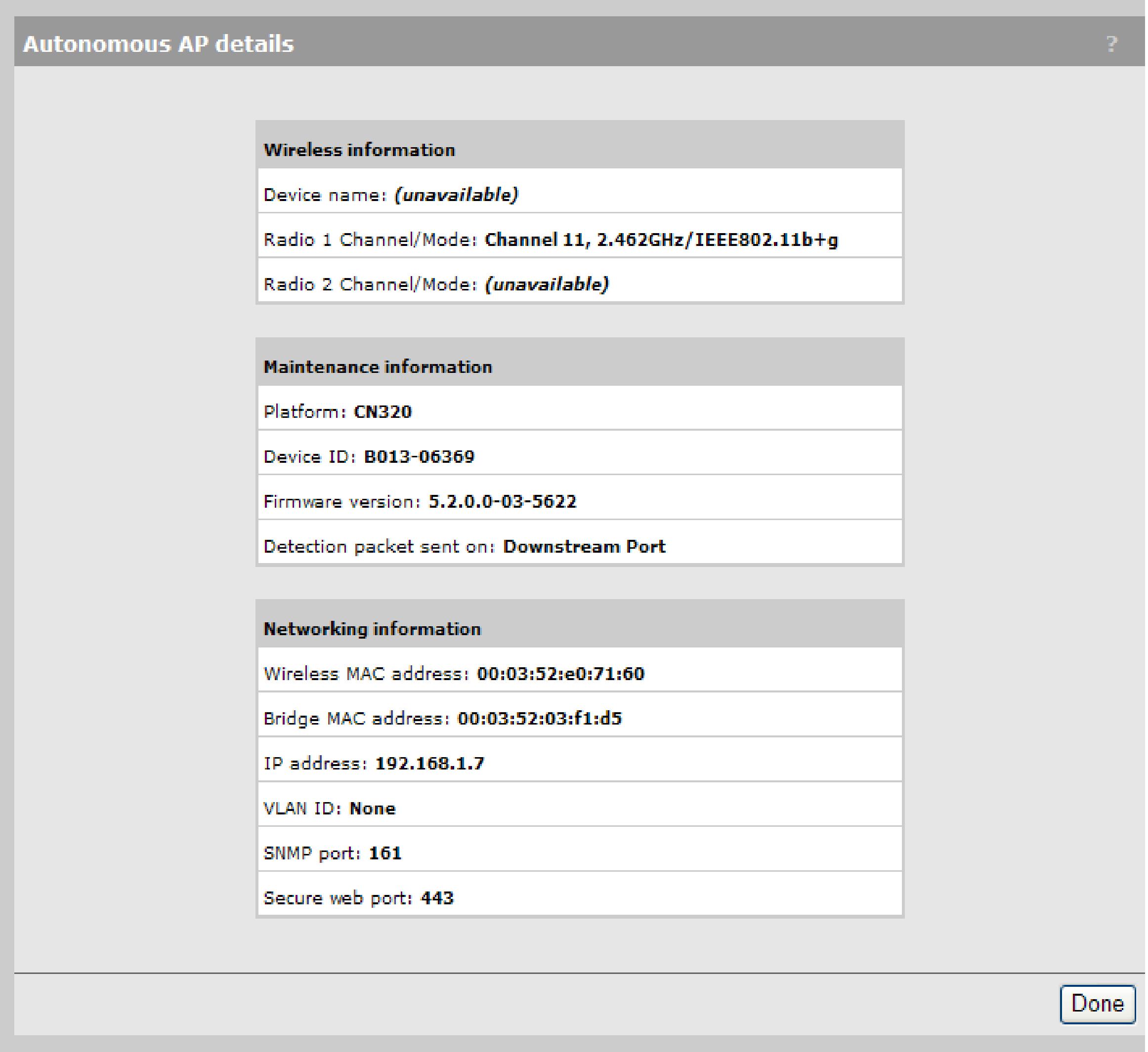
Number of detected autonomous APs: 1

Device ID	Wireless MAC address	Device MAC address	IP address	Device name	Channel(s)
B058-00291	00:03:52:c7:dd:a0	00:03:52:07:04:4c	192.168.1.11	*(unavailable)*	Channel 4, 2.427GHz

XML version (For use as a firmware distribution list.)

Figure 13-1: Autonomous APs Window

As shown in the above image, the **Summary** list includes a **Detected** link and count in the **Summary** list, and the **Network Tree** includes an **Autonomous APs** branch on **Service Controller**. These elements only appear when at least one autonomous APs has been detected. As shown, when Autonomous APs is selected, the list of **Detected Autonomous APs** list appears in the right pane. Click a link in the **Device ID** column to display the **Autonomous APs details** like this:



Autonomous AP details

Wireless information

Device name: ***(unavailable)***

Radio 1 Channel/Mode: **Channel 11, 2.462GHz/IEEE802.11b+g**

Radio 2 Channel/Mode: ***(unavailable)***

Maintenance information

Platform: **CN320**

Device ID: **B013-06369**

Firmware version: **5.2.0.0-03-5622**

Detection packet sent on: **Downstream Port**

Networking information

Wireless MAC address: **00:03:52:e0:71:60**

Bridge MAC address: **00:03:52:03:f1:d5**

IP address: **192.168.1.7**

VLAN ID: **None**

SNMP port: **161**

Secure web port: **443**

Figure 13-2: Autonomous APs Details

You can also click the link in **IP address** column to launch the AP’s management tool. Refer to the *Wi² AP Admin Guide* for details.

13.1.3 Firmware Distribution

In simple topologies, the service controller is able to distribute firmware to one or more autonomous APs as described in “Firmware Distribution” on page 349.

13.1.4 Switching a Controlled AP to Autonomous Mode

To switch a controlled AP to autonomous mode, select the AP in the **Default Group** branch of the Network Tree, and then in the right pane select **Maintenance** > **System** and select **Switch to Autonomous Mode**.

NOTE

The AP will restart and lose all configuration settings received from the service controller, returning to its default configuration. You can then configure it via its management tool.

13.2 Configuring Autonomous APs

Autonomous APs must be configured via their own management tool. For convenience, you can launch an autonomous AP’s management tool from within the service controller’s management tool by clicking the link in the IP address column of the Detected Autonomous APs page. (Providing network access is possible.)

When connecting one or more autonomous APs to co-exist with a service controller, some configuration issues must be addressed to ensure that data traffic and management traffic is able to flow between both devices.

If the management computer connects to the AP through the service controller’s Internet port but the AP connects via the LAN port, static NAT mappings will be needed to be created to allow traffic to go through the service controller’s firewall. Refer to the *Wi² AP Admin Guide*.

13.2.1 Virtual Network Definitions

Although the service controller cannot configure autonomous APs, the APs can work with the service controller to benefit from the advanced access control services a service controller provides. To do this, use the autonomous AP’s management tool to configure virtual networks that use the same SSID and/or VLAN as already configured on the service controller. The matching virtual network configuration is illustrated as follows:

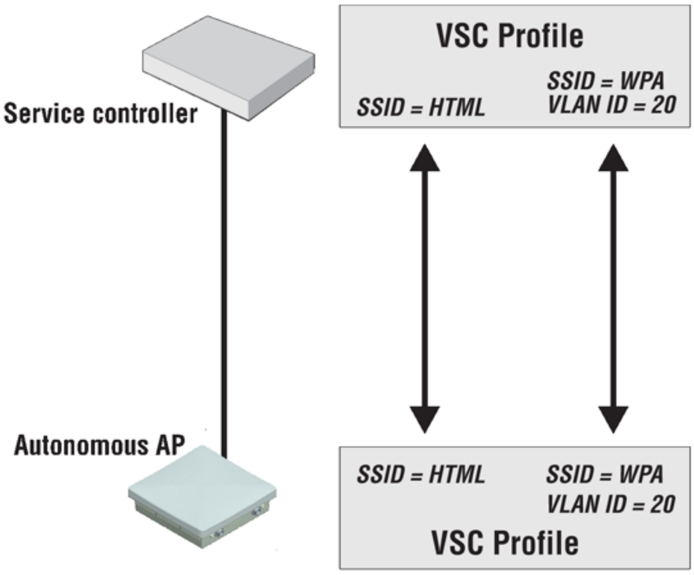


Figure 13-3: Matching Virtual Network Configuration

13.2.1.1 Management with VLANs

When operating in a VLAN environment, management traffic can be carried on its own VLAN. Configure the virtual network on both the autonomous AP and the service controller as illustrated here:

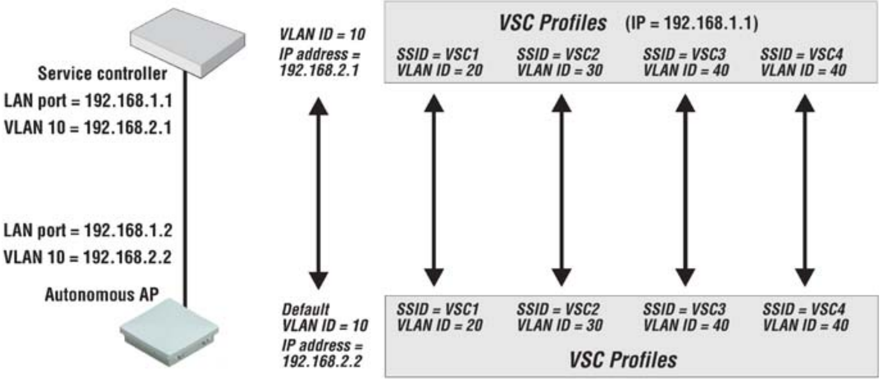


Figure 13-4: Configuration of the Virtual Network on the Autonomous AP and the Service Controller

In this example, the traffic for each wireless network is carried on its own VLAN. This leaves only management traffic from the autonomous AP on VLAN 10 segment. A static IP is assigned on both ends to permit the two devices to communicate.

13.3 Working with Third-party Autonomous APs

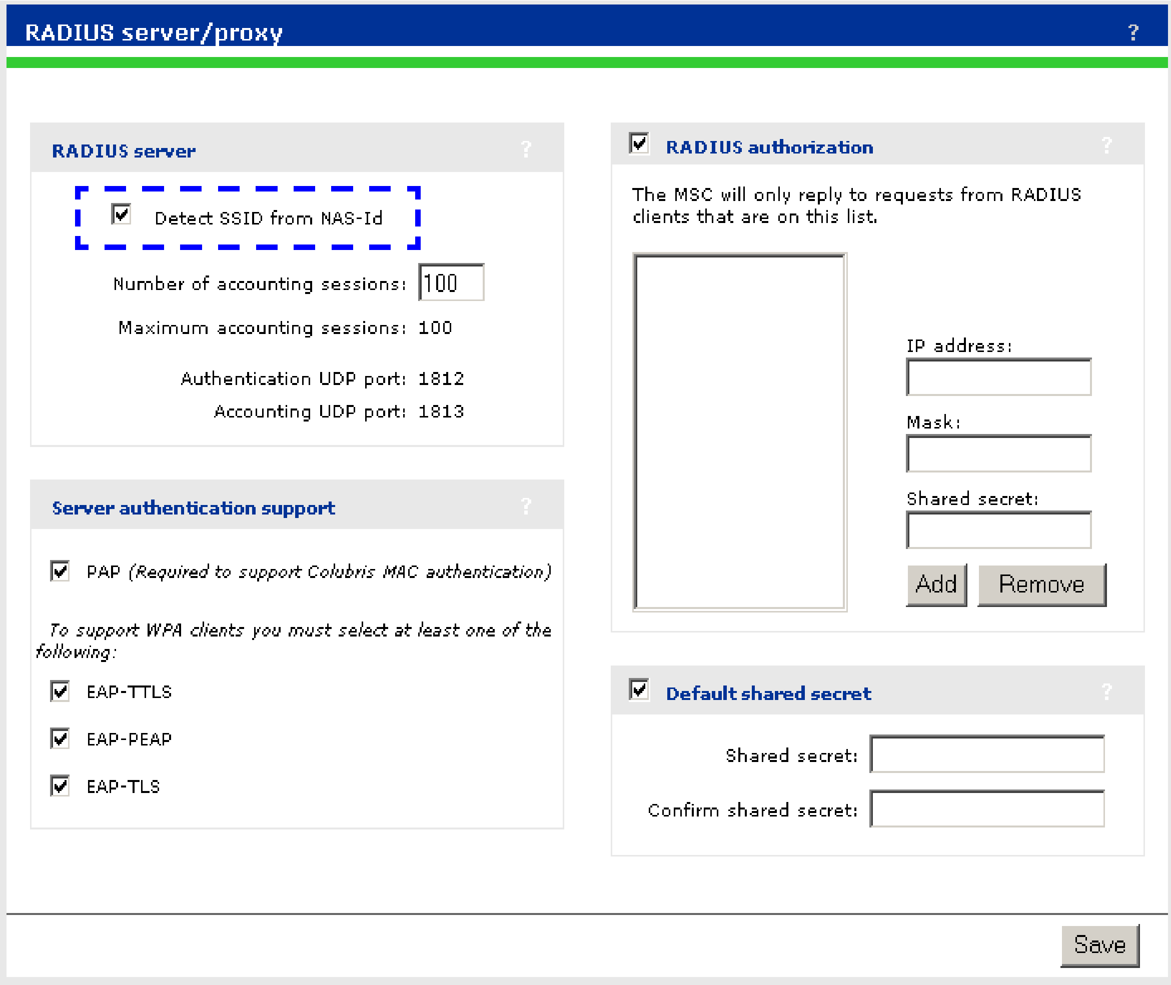
Third-party APs can be used with a service controller with both access controlled and non-access controlled virtual networks.

13.3.1 Virtual Network Selection

User traffic from third-party APs is mapped to a virtual network on the service controller in the same way as for Alvarion APs. Refer to “Using Multiple Virtual Networks” on page 125 for details. This means that traffic is assigned to the default virtual network, unless it is on a VLAN, in which case it is assigned to the virtual network with matching VLAN ingress definition.

Because the Alvarion location-aware feature is not available on third-party APs, support for virtual network selection using an SSID requires that the following additional configuration be performed:

- Configure the AP to send its SSID as the NAS ID in all **authentication and accounting** requests.
- Enable the **Detect SSID from NAS-Id** option on the **Service controller >> Security > RADIUS server** page.



RADIUS server/proxy

RADIUS server

☑ Detect SSID from NAS-Id

Number of accounting sessions: 100

Maximum accounting sessions: 100

Authentication UDP port: 1812

Accounting UDP port: 1813

Server authentication support

☑ PAP *(Required to support Colubris MAC authentication)*

To support WPA clients you must select at least one of the following:

☑ EAP-TTLS

☑ EAP-PEAP

☑ EAP-TLS

☑ RADIUS authorization

The MSC will only reply to requests from RADIUS clients that are on this list.

IP address:

Mask:

Shared secret:

☑ Default shared secret

Shared secret:

Confirm shared secret:

Figure 13-5: Virtual Network Selection

14

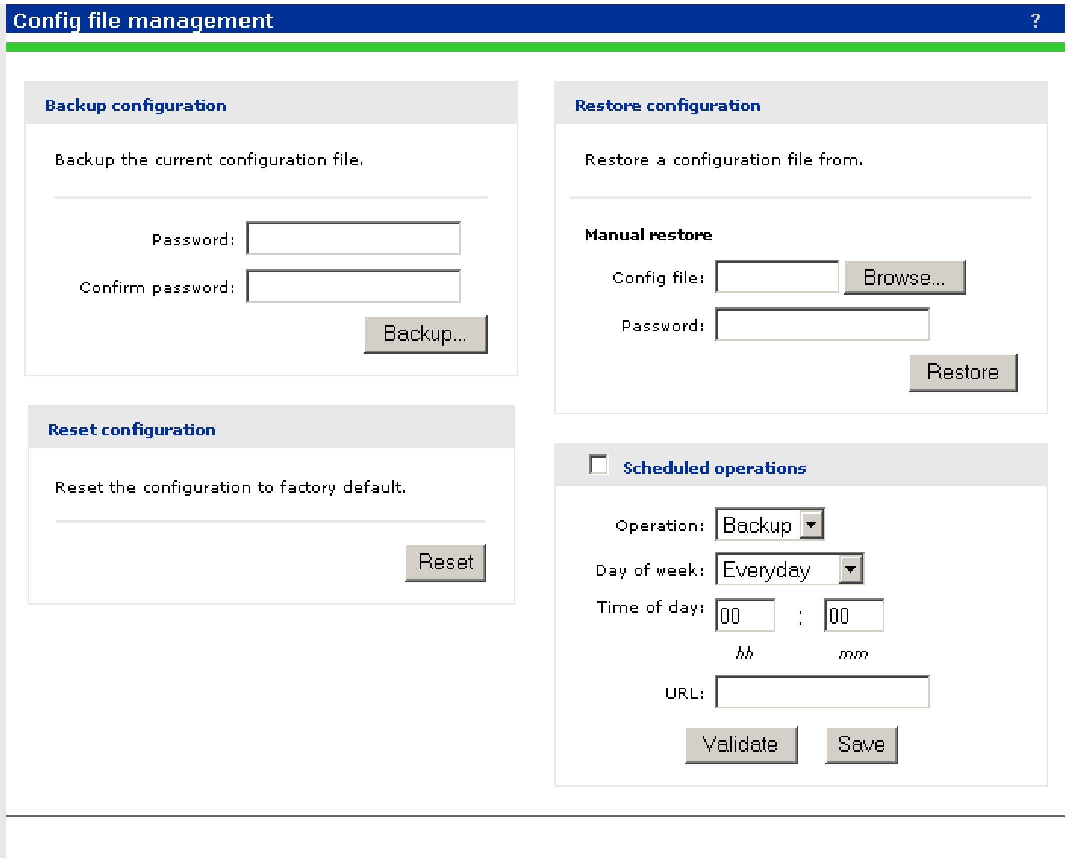
Chapter 14 - Maintenance

In This Chapter:

14.1 Config File Management

The configuration file contains all the settings that customize the operation of the service controller. You can save and restore the configuration file manually, automatically, or with a tool like cURL (explained later in this chapter).

Select **Maintenance > Config file management**.



Backup the current configuration file.

Restore a configuration file from.

Reset the configuration to factory default.

Operation: Backup

Day of week: Everyday

Time of day: 00 : 00

Figure 14-1: Config File Management

14.1.1 Manual Configuration File Management

The following options are available for manual configuration file management.

14.1.1.1 Backup Configuration

The **Backup configuration** group box enables you to back up your configuration settings so that they can be easily restored in case of failure. You can also use this option if you want to directly edit the configuration file.

Before you install new firmware, you should always back up your current configuration. Select **Backup** to start the process. You are prompted for the location in which to save the configuration file.

If you specify a **Password,** the configuration file is protected by encrypting sensitive fields (example, passwords, secrets, and certificates) with a key based on the password. See also Restore Configuration below.

NOTE

Even without a password, the certificates are still encrypted but with a key that is identical on all devices.

NOTE

The local username and password for the administrator are not saved to the backup configuration file. If you upload a configuration file, the current username and password are not overwritten.

NOTE

Local user accounts are backed up but are not encrypted.

14.1.1.2 Reset Configuration

See "Resetting to Factory Defaults" on page 359.

14.1.1.3 Restore Configuration

The **Restore configuration** group box enables you to reload a previously saved backup configuration file.

This feature enables you to maintain several configuration files with different settings, which can be useful if you must frequently alter the configuration of the service controller or if you are managing several service controllers from a central site.

Use the following steps to restore a saved configuration file.

1 Select **Maintenance > Config file management.** The **Config file management** page opens.

2 In the **Restore configuration** group box under **Manual restore,** select **Browse** to navigate to and select the configuration file that you want to restore.

3 If the configuration file is protected with a password (see Backup Configuration) you must supply the correct password to restore the complete

configuration. If you supply an invalid password, all settings are restored except the certificates.

4 To upload the selected file to the service controller, select **Restore.**

NOTE

The service controller automatically restarts when the upload is complete.

14.1.2 Scheduled Operations

The **Scheduled operations** group box enables you to schedule unattended backups or restorations of the service controller's configuration file. See also "Scheduled Update" on page 342.

Use the following steps to schedule a backup or restoration of the service controller's configuration file.

1 Select **Maintenance > Config file management.** The **Config file management** page opens.

2 At lower right, select the **Scheduled operations** checkbox.

3 Under **Operation,** select **Backup** or **Restore**.

4 Under **Day of week,** select **Everyday,** or select a specific day of the week on which to perform the backup or restoration.

5 Under **Time of day,** specify the hour and minute on which to perform the backup or restoration. Use the format *hh mm,* where

- *hh* ranges from 00 to 23
- *mm* ranges from 00 to 59

6 Under **URL,** specify the path that leads to the remote directory in which to save the configuration file or from which to load the configuration file. For example:

- **ftp://username:password@192.168.132.11/new.cfg**
- **http://192.168.132.11/new.cfg**

7 To confirm that the specified **URL** is correct, select **Validate.**

8 To commit the schedule that you have configured, select **Save.**

14.1.3 Managing the Configuration File with cURL

NOTE

This is an advanced topic. It is recommended that you perform configuration file management as described in the immediately-previous sections Manual Configuration File Management or Scheduled Operations.

You can perform configuration-file-related tasks using the free tool cURL (http://curl.haxx.se/), version 7.1.0 or higher.

The following cURL commands shows you how to manage the configuration file. The following setup is assumed:

- IP address of the service controller Internet port is 24.28.15.22.
- Management access to the Internet port is enabled.
- Configuration file is **new.cfg**.

These examples are not secure—that is, no certificates are used for authentication—but data traffic is encrypted.

NOTE

To secure the connection with the service controller using certificates, use the **--cacert** option to specify where the CA certificates are located on your computer. You must also specify the host name **wireless.alvarion.com** instead of using an IP address. The host name must be resolved either by using a DNS server or using the hosts file on your computer.

NOTE

The first time an AP is started up after a factory reset, the end user license agreement must be accepted and the country of operation must be set. This must be done manually or be modifying the sample cURL scripts in this section.

14.1.3.1 Uploading the Configuration File

1. Prepare the service controller to receive the login.

```
curl -s -k "https://24.28.15.22/home.asp"
```

2. Log in to the management interface.

```
curl -s -k --dump-header cookie.txt "https://24.28.15.22/goform/Logout" -d
username=admin
   -d pw=admin
```

3. Prepare the service controller to receive the configuration update.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/script/config_init.asp"
```

4 Upload the configuration file.

```
curl -s -k --cookie cookie.txt -F config=@new.cfg -F backup=Restore
"https://24.28.15.22/    goform/ScriptUploadConfig"
```

5 Reset the service controller to activate the new configuration.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/script/reset.asp"
Downloading the configuration file
```

1 Prepare the service controller to receive the login.

```
curl -s -k "https://24.28.15.22/home.asp"
```

2 Log in to the management interface.

```
curl -s -k --dump-header cookie.txt "https://24.28.15.22/goform/Logout" -d
username=admin
   -d pw=admin
```

3 Prepare the configuration file for download.

```
curl -s -k --cookie cookie.txt
"https://24.28.15.22/goform/FormBackupConfig"   -d backup=Backup
```

4 Download the configuration file.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/download/new.cfg" -o new.cfg
```

5 Log out.

```
curl -s -k --cookie cookie.txt “https://24.28.15.22/goform/Logout” -d
logout=Logout
```

14.1.3.2 Resetting the Configuration to Factory Defaults

See also “Resetting to Factory Defaults” on page 359.

1 Prepare the service controller to receive the login.

```
curl -s -k "https://24.28.15.22/home.asp"
```

2 Log in to the management interface.

```
curl -s -k --dump-header cookie.txt "https://24.28.15.22/goform/Logout" -d
username=admin
   -d pw=admin
```

3 Reset configuration to factory defaults.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/goform/
ScriptResetFactory?reset=Reset+to+Factory+Default"
```

4 Reset the service controller to activate the new configuration.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/script/reset.asp"
```

14.2 Firmware Updates

CAUTION

Be sure to check for other update issues in the new firmware Release Notes.

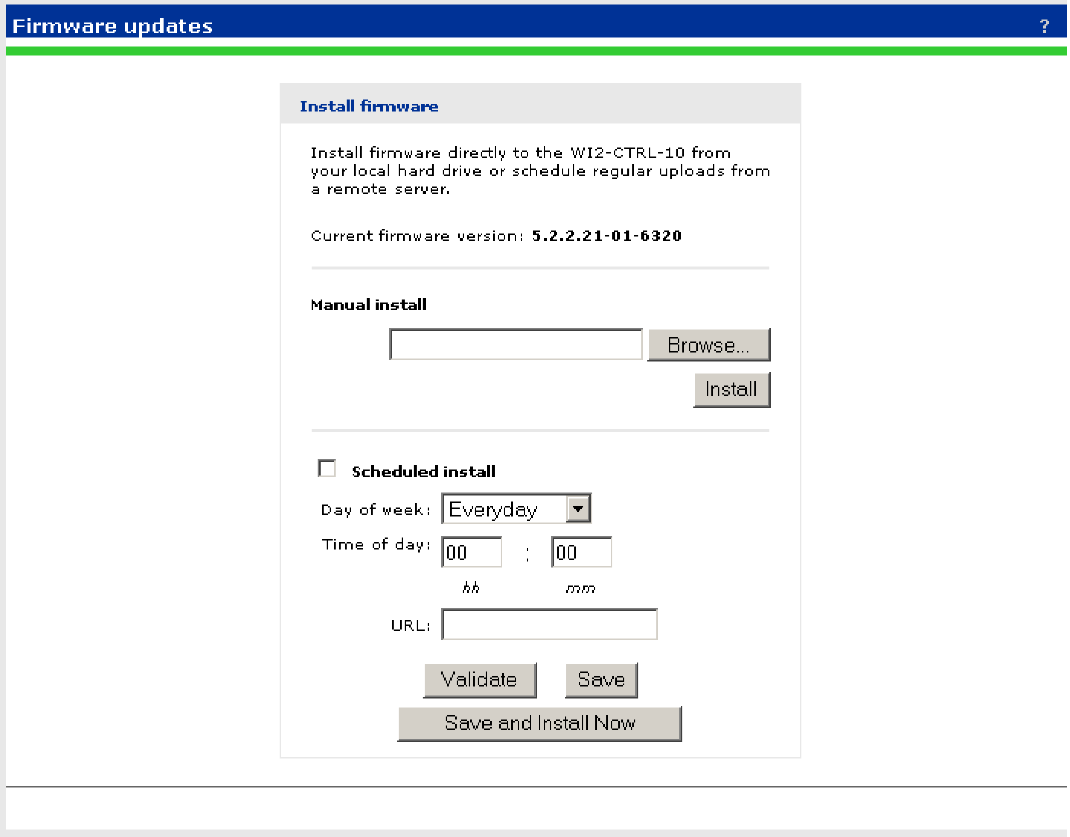
CAUTION

After updating the service controller **firmware, controlled APs are automatically updated to the same version that is installed on the service controller. This causes the APs to restart. To minimize network disruption, use the scheduled install option to have upgrades performed outside of peak usage hours.**

NOTE

Configuration settings are preserved during firmware upgrades.

To update service controller firmware, select **Maintenance** > **Firmware updates**.



Firmware updates

Install firmware

Install firmware directly to the WI2-CTRL-10 from your local hard drive or schedule regular uploads from a remote server.

Current firmware version: **5.2.2.21-01-6320**

Manual install

□ Scheduled install

Day of week: Everyday

Time of day: 00 : 00

hh mm

URL:

Figure 14-2: Firmware Updates

14.2.1 Immediate Update

To update the service controller firmware now, **Browse** to the firmware file (extension .cim) and then select **Install.**

NOTE

At the end of the firmware-update process, the service controller and all controlled APs automatically restart, causing all users to be disconnected. Once the service controller and APs resume operation, all users must reconnect.

14.2.2 Scheduled Update

The service controller can automatically retrieve and install firmware from a remote web site identified by its URL.

To schedule firmware installation, follow this procedure:

1 Enable **Scheduled install**.

2 For **Day of week** select a specific day or **Everyday** and set **Time of day**.

3 For **URL**, specify an ftp or http address like this:

- » **ftp://username:password@192.168.132.11/newfirmware.cim**
- » **http://192.168.132.11/newfirmware.cim**

4 **Validate** the URL.

5 To commit the schedule, select **Save.**

6 Or, to commit the schedule and also update the firmware immediately, select **Save and Install Now**.

NOTE

At the end of the firmware-update process, the service controller automatically restarts, causing all users to be disconnected. Once the service controller resumes operation, all users must reconnect.

NOTE

Before a scheduled firmware update is performed, only the first few bytes of the firmware file are downloaded to determine if the firmware is newer than the current. If it is not, the download stops and the firmware is not updated at this time. Which means that if by accident you try to upload the same firmware, it will not affect the operation of your network.

14.2.3 Updating Firmware with cURL

NOTE

This is an advanced topic. It is recommended that you upgrade firmware as described in the immediately-previous sections Immediate Update or Scheduled Update.

You can perform firmware-update-related tasks using the free tool cURL (http://curl.haxx.se/), version 7.1.0 or higher.

The following cURL commands shows you how to manage the firmware file. The following setup is assumed:

- IP address of the service controller Internet port is 24.28.15.22.
- Management access to the Internet port is enabled.
- Firmware file is **newfirmware.cim**.

Upload the firmware as follows:

1 Prepare the service controller to receive the login.

```
curl -s -k "https://24.28.15.22/home.asp"
```

2 Log in to the management interface.

```
curl -s -k --dump-header cookie.txt "https://24.28.15.22/goform/Logout" -d
username=admin
-d pw=admin
```

3 Prepare the service controller to receive the firmware update.

```
curl -s -k --cookie cookie.txt "https://24.28.15.22/script/firmware_init.asp"
```

4 Upload the firmware. Once the upload is complete the service controller will automatically restart.

```
curl -s -k --cookie cookie.txt -F firmware=@newfirmware.cim -F backup=Install
"https://24.28.15.22/   goform/ScriptUploadFirmware"
```

14.3 Licenses

Some service controller features are activated by installation of optional licenses. For example, the Layer 2 and Layer 3 mobility feature requires the optional AOS Mobility Pack license. Such features are only enabled when a valid license is installed.

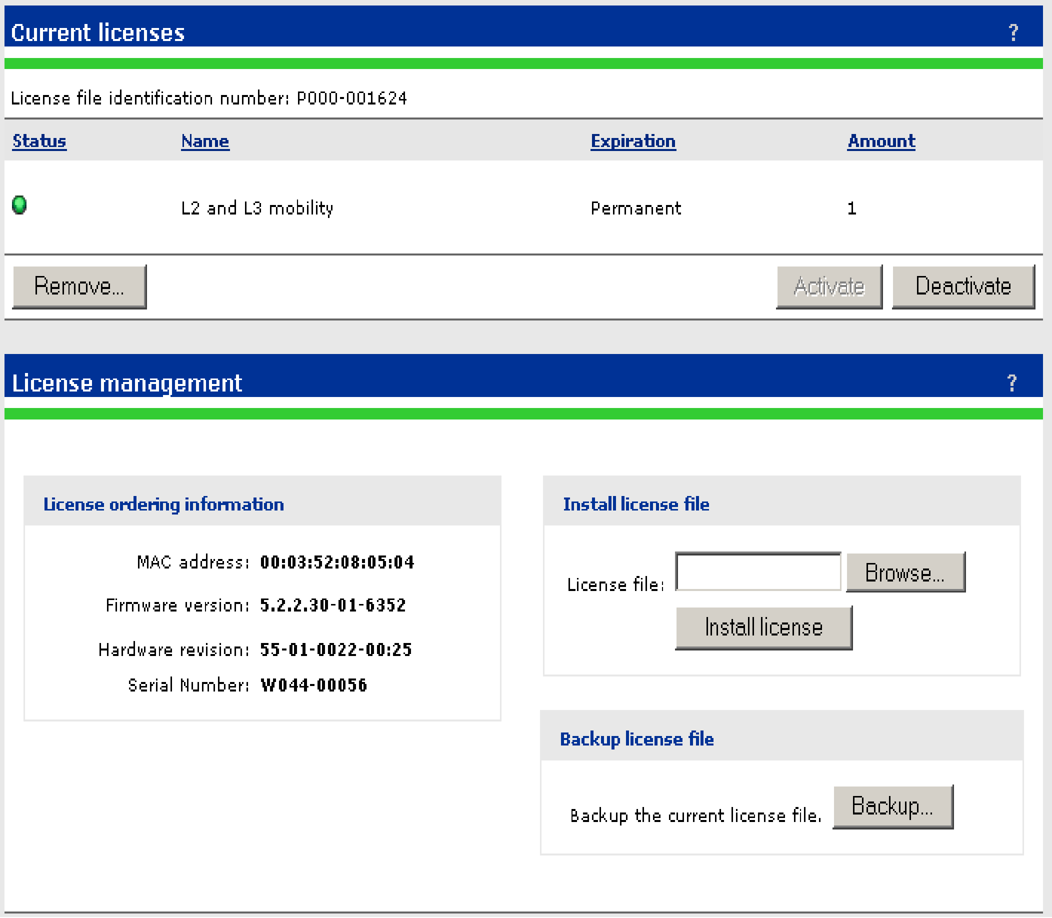
NOTE

When working with controlled APs, AP feature licenses are automatically distributed to the affected APs.

If you purchased an optional-feature license at original service controller purchase time, the license is factory-installed.

Feature licenses purchased later must be installed manually.

Select **Maintenance > Licenses**. In this example, license **L2 and L3 mobility** was factory installed.



Current licenses

License file identification number: P000-001624

Status	Name	Expiration	Amount
●	L2 and L3 mobility	Permanent	1

License management

License ordering information

MAC address: **00:03:52:08:05:04**

Firmware version: **5.2.2.30-01-6352**

Hardware revision: **55-01-0022-00:25**

Serial Number: **W044-00056**

Install license file

License file:

Backup license file

Backup the current license file.

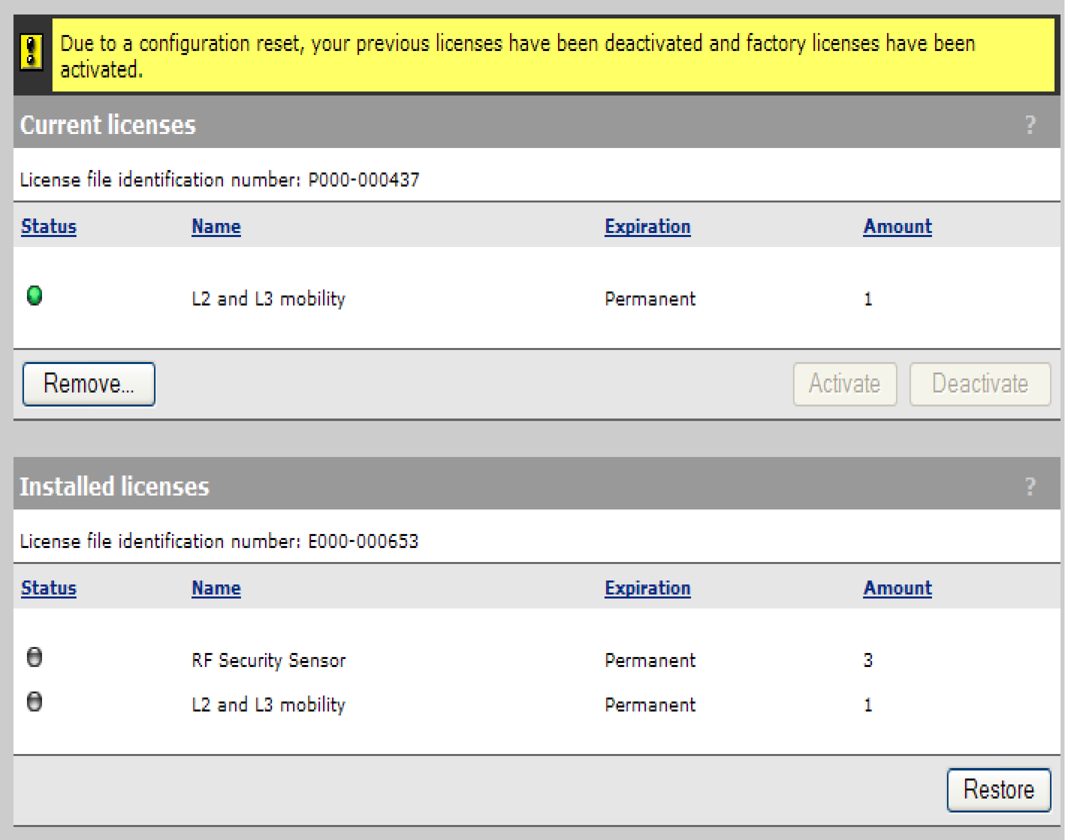
Figure 14-3: Current Licenses

Work with licenses as follows:

- To temporarily deactivate all licenses, select **Deactivate**. Later, select **Activate** to reactivate them.
- To remove all licenses, select **Remove** and then at the prompt, select **OK**.
- Before removing licenses, be sure to first backup the license file to your hard drive, using the **Backup** button.
- To order a new feature license, provide all information in the **License ordering information** box to your vendor.
- To install a license file, **Browse** to the file and then select **Install License**.
- To backup all licenses into a single file, select **Backup**.

14.3.0.1 Factory Reset Considerations

After a factory reset, factory-installed licenses are automatically re-activated but user-installed licenses remain in a deactivated state until manually activated. This is done to ensure a true factory-default reset. As shown here, automatically-reactivated factory-installed licenses are shown in the **Current licenses** table. All licenses are shown in the new **Installed licenses** table.



Due to a configuration reset, your previous licenses have been deactivated and factory licenses have been activated.

Current licenses

License file identification number: P000-000437

Status	Name	Expiration	Amount
●	L2 and L3 mobility	Permanent	1

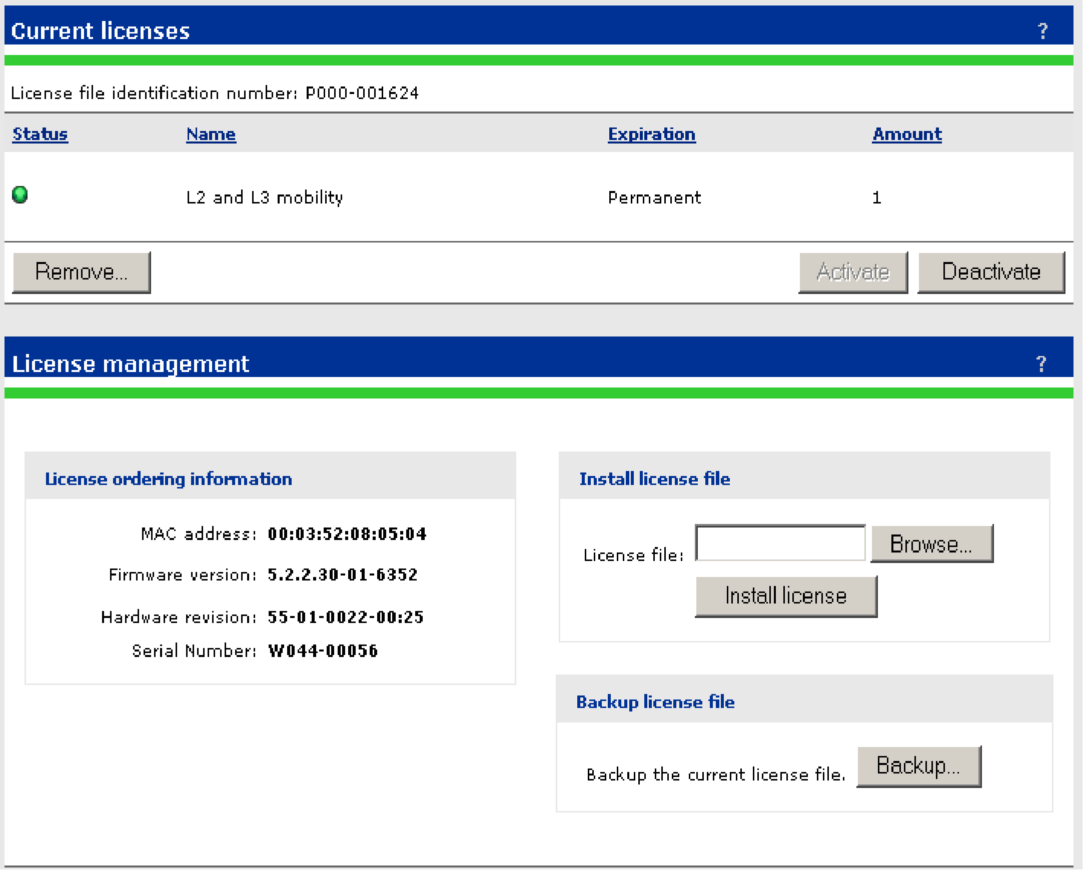
Installed licenses

License file identification number: E000-000653

Status	Name	Expiration	Amount
●	RF Security Sensor	Permanent	3
●	L2 and L3 mobility	Permanent	1

Figure 14-4: Licenses

To activate all user-installed licenses, select the **Restore** button. Table **Controlled licenses** is updated to include the user-installed licenses and the **Installed licenses** table disappears.



License file identification number: P000-001624

Status	Name	Expiration	Amount
●	L2 and L3 mobility	Permanent	1

License ordering information

MAC address: **00:03:52:08:05:04**

Firmware version: **5.2.2.30-01-6352**

Hardware revision: **55-01-0022-00:25**

Serial Number: **W044-00056**

Install license file

License file:

Backup license file

Backup the current license file.

Figure 14-5: Current Licenses

14.4 Firmware Distribution

NOTE

This information **ONLY APPLIES TO AUTONOMOUS APs**. Controlled APs automatically receive their firmware from the service controller.

NOTE

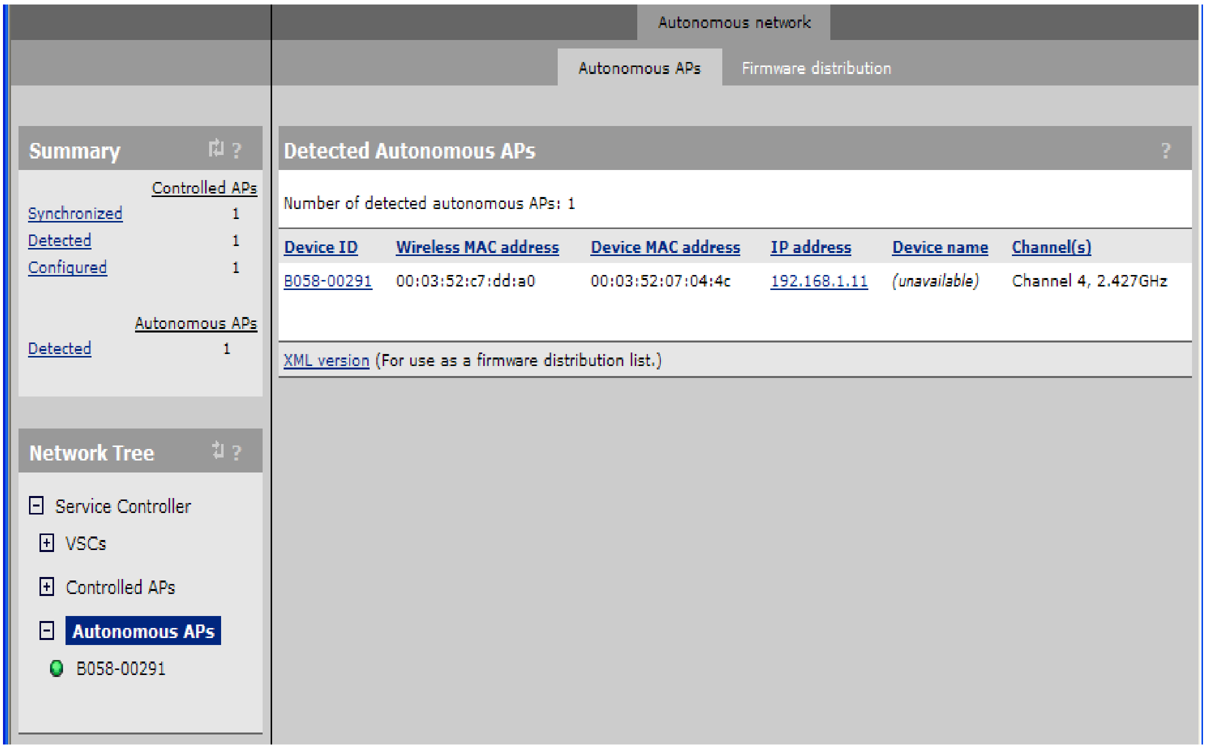
To support firmware distribution, automonous APs must have access to their management tool enabled (on the **Management > Management tool** page).

The firmware distribution feature enables you to use the service controller to automatically install new firmware on one or more autonomous APs even though such APs are not controlled by the service controller.

NOTE

This is the preferred method for upgrading the firmware on autonomous APs.

Select **Autonomous APs** in the Network Tree. The **Detected Autonomous APs** page opens.



Summary

	Controlled APs
Synchronized	1
Detected	1
Configured	1

	Autonomous APs
Detected	1

Detected Autonomous APs

Number of detected autonomous APs: 1

Device ID	Wireless MAC address	Device MAC address	IP address	Device name	Channel(s)
B058-00291	00:03:52:c7:dd:a0	00:03:52:07:04:4c	192.168.1.11	*(unavailable)*	Channel 4, 2.427GHz

XML version (For use as a firmware distribution list.)

Figure 14-6: Detect Autonomous APs

NOTE

Make sure that CDP is enabled on all autonomous APs. This ensures that they will all be visible to the service controller.

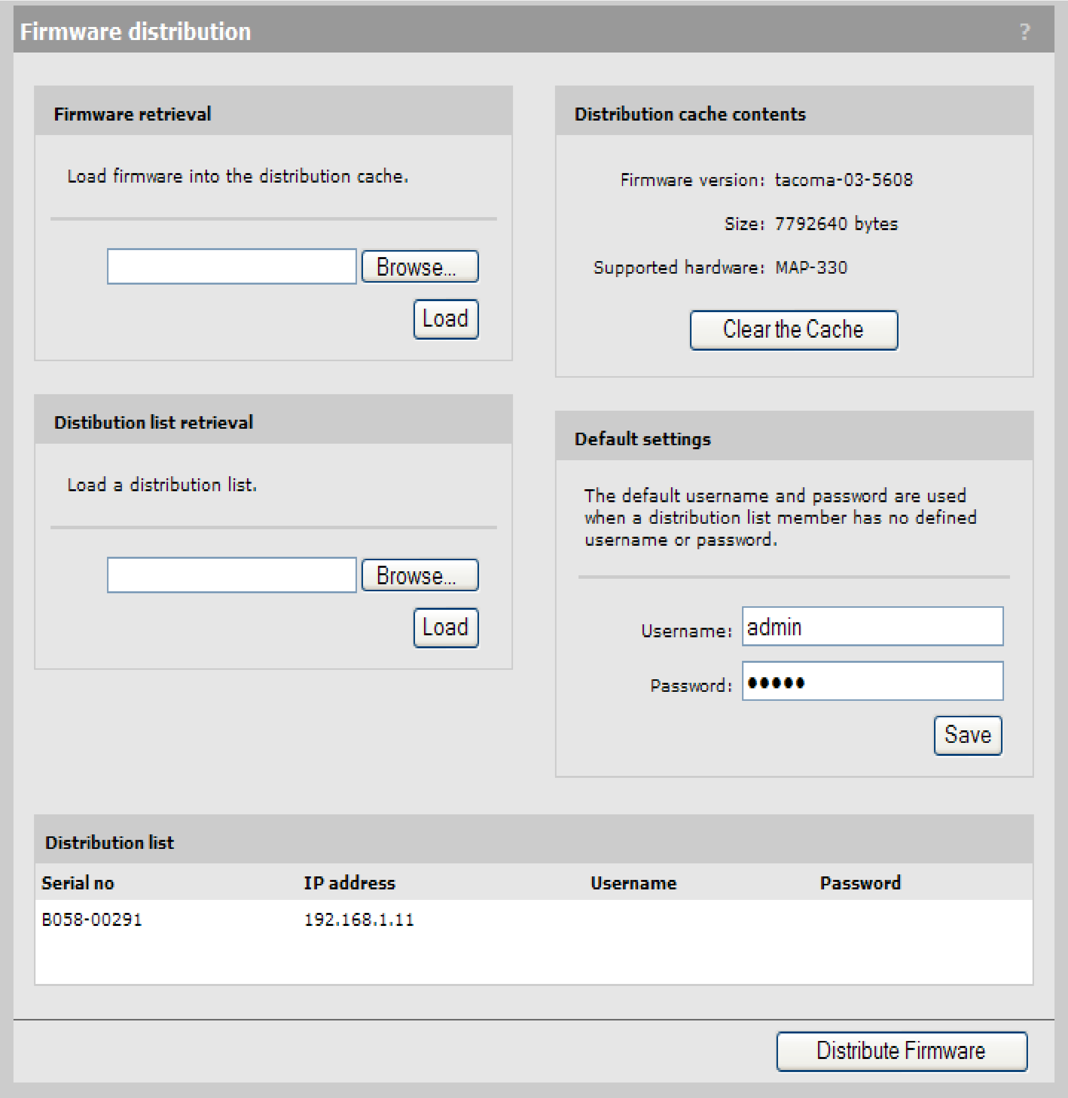
To distribute firmware to these APs, follow this procedure:

1 At the bottom of the **Detected Autonomous APs** page select the **XML version** link. An XML-based firmware distribution list is auto-generated and displayed in your web browser.

2 Use your web browser's **File** > **Save A**s feature to save the XML file on your computer.

3 In the Network Tree, select **Autonomous APs** >> **Autonomous network** > **Firmware distribution**.

4 In the **Firmware retrieval** box, browse to the firmware file corresponding to the autonomous AP model and select **Load**. The firmware file is loaded into the service controller cache and the **Distribution cache contents** is updated. This example shows firmware loaded for an AP-330.



Firmware distribution

Firmware retrieval

Load firmware into the distribution cache.

Distribution cache contents

Firmware version: tacoma-03-5608

Size: 7792640 bytes

Supported hardware: MAP-330

Distibution list retrieval

Load a distribution list.

Default settings

The default username and password are used when a distribution list member has no defined username or password.

Username: admin

Password: ●●●●●

Distribution list

Serial no	IP address	Username	Password
B058-00291	192.168.1.11		

Figure 14-7: Firmware Distribution

NOTE

If you intend to upgrade different APs models, you must distribute to each model separately because only one firmware image can be stored in the cache at a time.

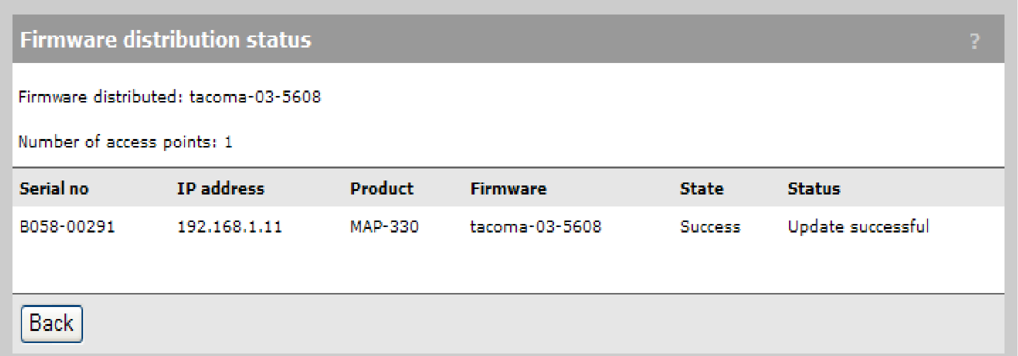
5 In the **Distribution list retrieval** box, browse to the XML file you saved in step 2 above and select **Load**. The XML file is processed and each AP it identifies is listed in the **Distribution list**.

NOTE

If you do not wish to distribute firmware to EVERY AP identified in the XML file, or the APs do not all have the same administrator username and password, you will need to manually edit the file to remove undesired APs and to possibly adjust usernames and password. See Optionally Edit the Distribution List below for details. You can edit the distribution list and reload it into the service controller.

6 Once the **Distribution list** contains the precise list of APs to which you want to distribute firmware, click the **Distribute Firmware** button. The firmware distribution process begins and the status page displays progress.

7 Occasionally click the web browser refresh button until **Status** shows **Update successful** for all APs.



Firmware distribution status

Firmware distributed: tacoma-03-5608

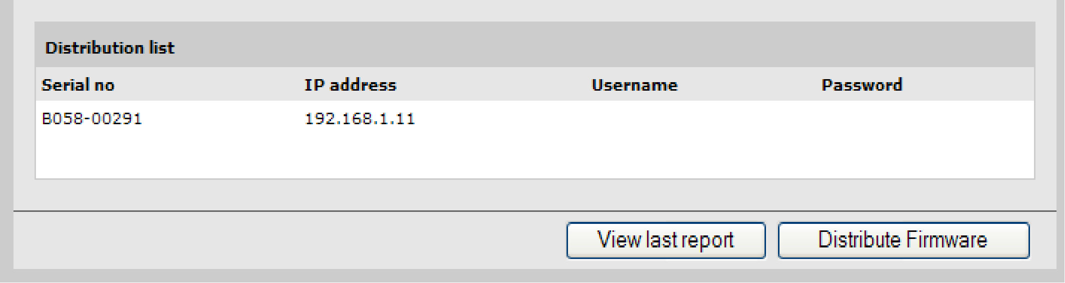
Number of access points: 1

Serial no	IP address	Product	Firmware	State	Status
B058-00291	192.168.1.11	MAP-330	tacoma-03-5608	Success	Update successful

Figure 14-8: Firmware Distribution Status

8 Click **Back** to return to the **Firmware distribution** page.

9 Later, you can select the **View last report** button at the bottom of the **Firmware distribution** page to re-display the most-recent firmware distribution status report.



Distribution list

Serial no	IP address	Username	Password
B058-00291	192.168.1.11		

Figure 14-9: Distribution List

14.4.1 Optionally Edit the Distribution List

You can edit the XML distribution list file generated via the **XML version** link of the **Detected Autonomous APs** page. For example, you can removed undesired APs or change usernames and passwords. Edit the XML file with a plain-text editor or an XML editor.

The XML entry for each AP is comprised of four fields:

- Serial number: Serial number of the target AP.
- IP address: IP address of the target AP.
- Username: Administrator username on the target AP.
- Password: Administrator password on the target AP.

Serial number and IP address are mandatory. Username and password fields are mandatory but values are optional. If all your autonomous APs have the same username and password, you can leave the username and password for every entry blank and instead specify them under **Default settings** on the Firmware distribution page.

The auto-generated XML file contains only the serial number and IP address of each AP, with empty username and password fields. Here is an example of an XML file including the optional username and password fields.

```
<serialno>C004-00100</serialno>
<ipaddress>192.168.130.160</ipaddress>
<username></username>
<password></password>
```

The username and password fields must always be specified, even if they are empty. For example:

```
<?xml version="1.0" ?>
<firmware-cache-distribution-list
xmlns="http://alvarion.com/firmwarecache">
  <access-points>
   <access-point>
      <serialno>R004-00003</serialno>
      <ipaddress>192.168.130.162</ipaddress>
      <username></username>
      <password></password>
    </access-point>
    <access-point>
      <serialno>M033-00004</serialno>
      <ipaddress>192.168.130.161</ipaddress>
```

```
            <username></username>
            <password></password>
          </access-point>
      </firmware-cache-distribution-list>
```

A

Appendix A - Regulatory Information

In This Appendix:

A.1 Regulatory Information

CAUTION

Changes or modifications not expressly approved by Alvarion for compliance could void the user's authority to operate the equipment.

The information in this Regulatory information appendix applies to products: Wi²-CTRL-10,
Wi²-CTRL-40, and Wi²-CTRL-200.

A.1.1 USA: Federal Communications Commission (FCC)

The Federal Communications Commission (in 47 CFR 15.105) has specified that the following notice be brought to the attention of the users of this product.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Cables used with this device must be properly shielded to comply with the requirements of the FCC Rules. Any changes or modifications to this equipment not expressly approved by the Alvarion Ltd. may cause harmful interference and void the FCC authorization to operate this equipment.

The end user of this product should be aware that any changes or modifications made to this equipment without the approval of Alvarion Ltd. could result in the product not meeting the Class A limits, in which case the FCC could void the user's authority to operate the equipment.

This equipment is compliant with FCC Part 15 DFS (Radar Avoidance).

A.1.2 Canada: Industry Canada (IC)

This Class A digital apparatus complies with Industry Canada Standard ICES-003 and
RSS210 Annex 9.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 et CNR-210 Annexe 9 d'Industrie Canada.

A.1.3 Europe: EU Declaration of Conformity

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

A.1.4 Declarations of Conformity

Alvarion Ltd.
21a HaBarzel St. PO Box 13139, Tel Aviv 69710, Israel.

Declares the following products:
Wi²-CTRL-10, Wi²-CTRL-40, and Wi²-CTRL-200 conform to the following standards:

A.1.4.1 European Directives and European Standards

EMC Directive 89/336 EEC	
Low Voltage Directive 73/23 EEC	
EN 60950-1	Safety
EN 55022: 1998+A1: 2000 (Class A)	
EN 61000-3-2:2000	
EN 61000-3-3: 1995+A1: 2001	

EN 55024: 1998;	IEC 61000-4-2: 1995+A1: 1998+ A2: 2000; IEC 61000-4-3: 1995+A1: 1998+ A2: 2000; IEC 61000-4-4: 1995+ A1: 2000; IEC 61000-4-5: 1995+A1: 2000;
	IEC 61000-4-6: 1996+A1: 2000;
	IEC 61000-4-8: 1993+A1: 2000;
	IEC 61000-4-11: 1994+A1: 2000

A.1.4.2 North American Standards

FCC Part 15-Subpart B (Class A)	Conducted Emission
FCC Part 15-Subpart B (Class A)	Radiated Emission
UL60950-1, CAN/CSA C22.2 No. 60950-1-03	Safety

B

Appendix B - Resetting to Factory Defaults

In This Appendix:

B.1 Introduction

To force a service controller into its factory default state, follow the procedures in this section.

CAUTION

Resetting a service controller to factory defaults deletes all configuration settings, resets the administrator username and password to “admin”, disables the DHCP server on the LAN port, sets the LAN port IP address to 192.168.1.1, and sets the Internet port to operate as a DHCP client.

NOTE

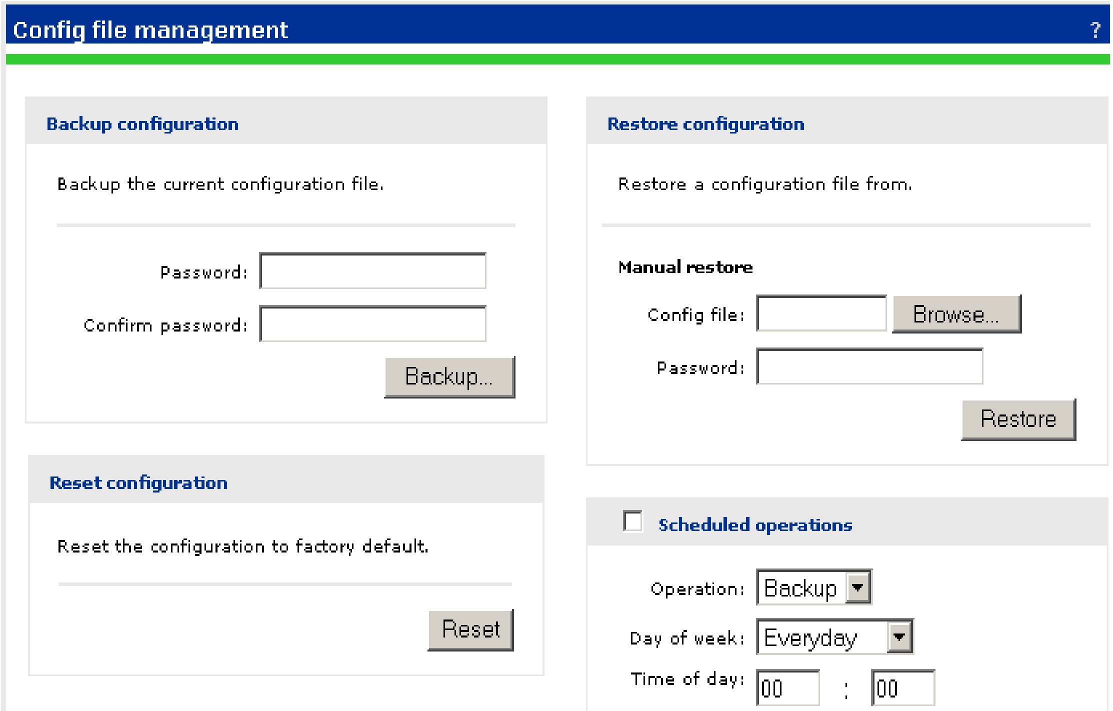
Licenses are retained after a factory reset. See “Factory Reset Considerations” on page 347.

B.1.1 Using the Reset SWITCH (Wi²-CTRL-10 only)

Using a tool such as a paper clip, press and hold the reset switch (back of Wi²-CTRL-10) for a few seconds until the front status lights flash three times.

B.1.2 Using the Management Tool

1. Launch the management tool (default https://192.168.1.1).
2. Select **Service Controller** (left pane), and then **Maintenance** > **Config file management**, and in section **Reset configuration**, select **Reset**.



Config file management ?

Backup configuration

Backup the current configuration file.

Password:

Confirm password:

Backup...

Restore configuration

Restore a configuration file from.

Manual restore

Config file: Browse...

Password:

Restore

Reset configuration

Reset the configuration to factory default.

Reset

□ Scheduled operations

Operation: Backup

Day of week: Everyday

Time of day: 00 : 00

Figure B-1: Config File Management

B.1.3 Using the Console (Serial) Port

Applies only to the Wi²-CTRL-40 and Wi²-CTRL-200.

It is recommended that you instead use the management tool as described previously. If, however, you forgot the administrator username or password, you can still force factory reset as described here:

1. Power off the service controller.
2. Connect a serial cable as described in the *Console port* section for your service controller in “Controller Hardware” on page 15.
3. Configure a communications terminal program such as Microsoft Hyperterminal for Windows or Minicom for Linux (http://alioth.debian.org/projects/minicom) as follows:

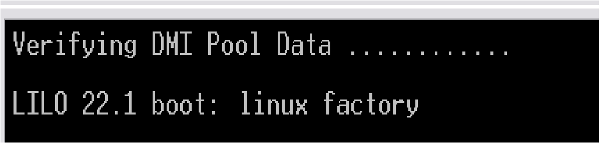
- **Speed**: For Wi²-CTRL-40, use 19200 bps, for Wi²-CTRL-200 use 115200 bps
- **Data bits**: 8
- **Parity**: none

- **Stop bits**: 1
- **Flow control**: none

4 Open an appropriately-configured terminal session.

5 Power on the service controller.

6 Wait for the memory test to complete and then press any keyboard key. After some boot information is displayed, the LILO prompt appears similar to this:



```
Verifying DMI Pool Data ............
LILO 22.1 boot:  linux factory
```

Figure B-2: LILO Prompt

7 Specify the command `linux factory` and press **Enter**. The factory reset commences.

8 Disconnect the serial cable.

C

Appendix C - DHCP Servers and Alvarion Vendor Classes

In This Appendix:

C.1 Overview

This section shows you how to configure the following DHCP servers to use the Alvarion vendor-specific class:

- "Windows Server 2003 Configuration"
- "ISC DHCP Server Configuration"

A vendor class allows certain devices to request specific information from a Dynamic Host Configuration Protocol server. Specifically, the Alvarion vendor class enables you to define a list of available service controllers to which APs operating in controlled mode can connect.

When DHCP clients send the Alvarion *vendor class identifier* in a DHCP request, a properly configured DHCP server returns the Alvarion-specific options defined on the server. These values are returned as DHCP option 43 (vendor-specific information) and can be interpreted only by a Alvarion device.

C.2 Windows Server 2003 Configuration

This section describes how to configure a Windows 2003 DHCP server to use the Alvarion vendor class.

The following procedure assumes that you have a Windows 2003 Server that has a DHCP server configured and running.

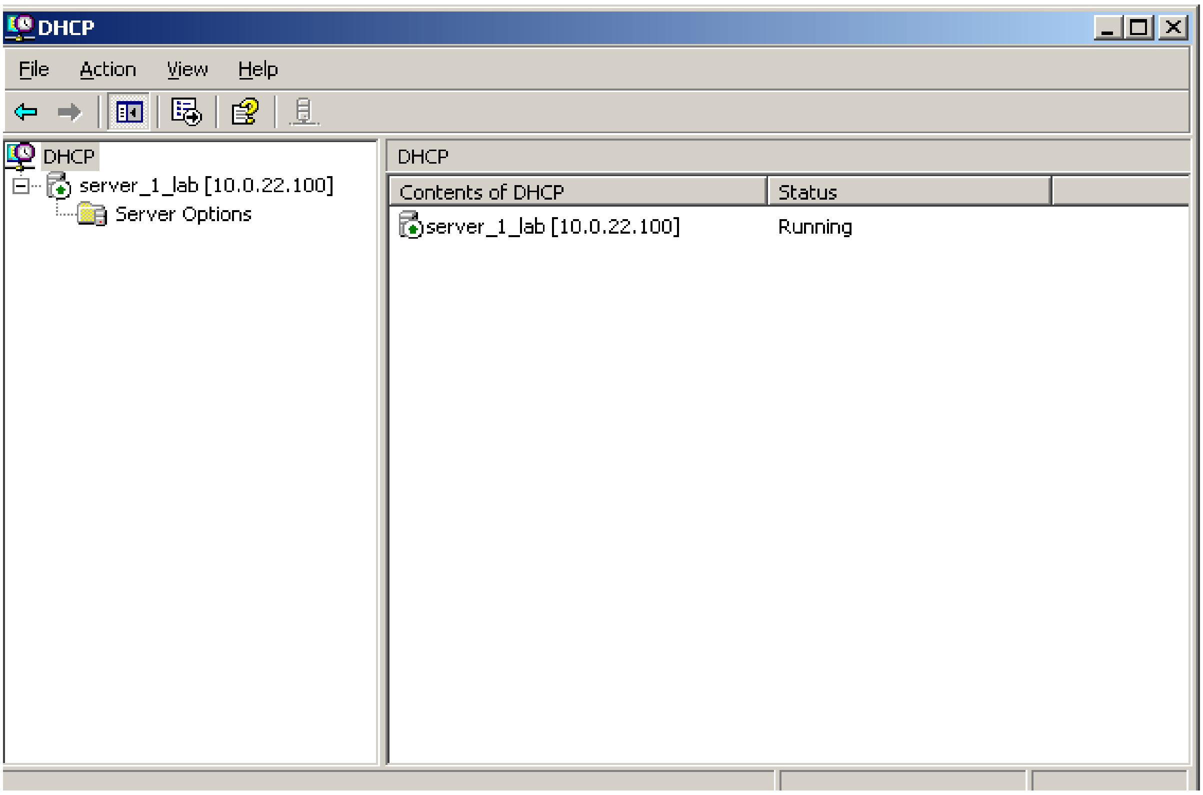
For more information see “Configuring Options and Classes on Windows Server” at

http://technet2.microsoft.com/WindowsServer/en/Library/d55609a5-2a1c-4f3f-ba8f-42b21828dc201033.mspx

C.2.1 Creating the Vendor Class

Use the following steps to create the Alvarion vendor class on the DHCP server.

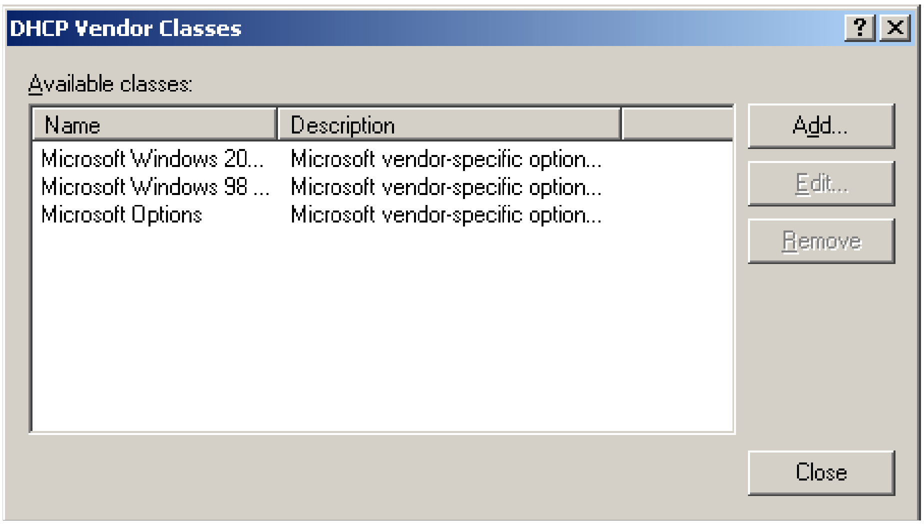
1 Select **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **DHCP.** The **DHCP** administration page opens.



Contents of DHCP	Status
server_1_lab [10.0.22.100]	Running

Figure C-1: DHCP Administration Page

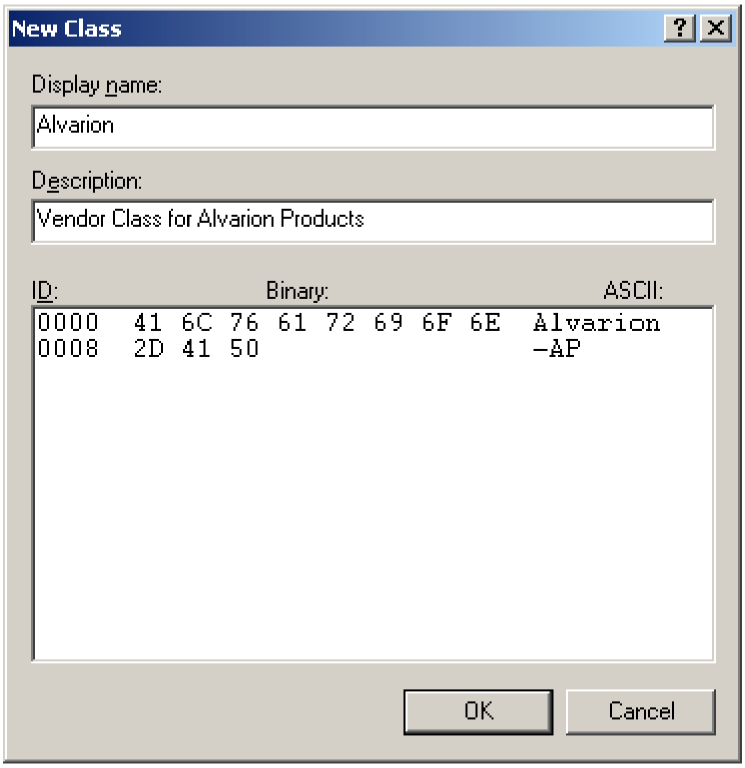
2 On the **DHCP** administration page in the navigation pane at left, select the name of the DHCP server to manage, and then select **Action** > **Define Vendor Classes.** The **DHCP Vendor Classes** page opens. Several default Microsoft vendor classes are preconfigured.



Name	Description
Microsoft Windows 20...	Microsoft vendor-specific option...
Microsoft Windows 98 ...	Microsoft vendor-specific option...
Microsoft Options	Microsoft vendor-specific option...

Figure C-2: DHCP Vendor Classes

3 On the **DHCP Vendor Classes** page, select **Add.** The **New Class** page opens.



Display name:
Alvarion

Description:
Vendor Class for Alvarion Products

```
ID:                 Binary:                    ASCII:
0000   41 6C 76 61 72 69 6F 6E   Alvarion
0008   2D 41 50                  -AP
```

Figure C-3: New Class

4 On the **New Class** page

» Under **Display name,** specify **Alvarion.**

» Under **Description,** specify any desired descriptive information for this vendor class.

» Select under **ASCII** and specify **Alvarion-AP.**

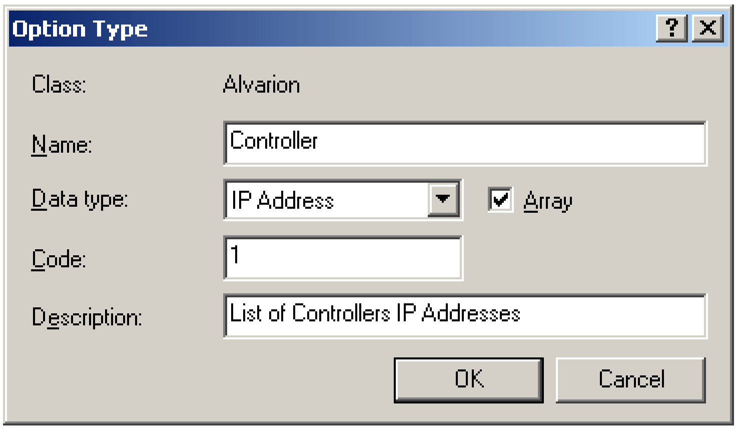
» Select **OK.**

5 The **New Class** page closes, and you return to the **DHCP Vendor Classes** page. To close the **DHCP Vendor Classes** page and return to the **DHCP** administration page, select **Close.**

C.2.2 Defining Vendor Class Options

Use the following steps to define Alvarion vendor class options on the DHCP server.

1 On the **DHCP** administration page, select **Action** > **Set Predefined Options.** From the **Option class** drop-down menu, select **Alvarion,** and then select **Add.** The **Option Type** page opens.



Class: Alvarion

Name: Controller

Data type: IP Address ☑ Array

Code: 1

Description: List of Controllers IP Addresses

Figure C-4: Defining Vendor Class Options

2 On the **Option Type** page,

» Under **Name,** specify **Controller.**

» Under **Data type,** select **IP Address** and enable the **Array** checkbox.

» Under **Code,** specify **1.**

» Under **Description,** specify **List of Controllers IP addresses.**

3 Select **OK** to close the **Option Type** page, and then select **OK** again to return to the **DHCP** administration page.

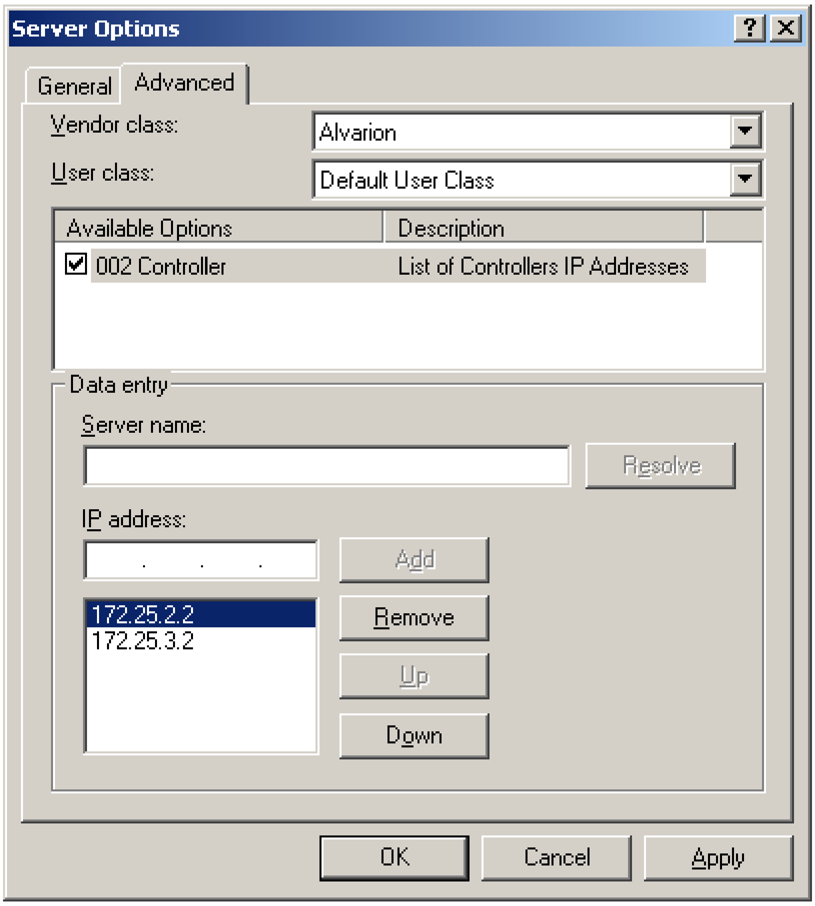
C.2.3 Applying the Vendor Class

After you define the Alvarion vendor class and its options, you can apply the class to specific Scopes or to the entire DHCP server. You must define the Alvarion vendor class for every Scope from which an AP can get an address.

Use the following steps to add the Alvarion vendor-specific option to one **Scope** on the DHCP server.

1 On the **DHCP** administration page, in the navigation pane, open the folder that corresponds to the desired **Scope.**

2 Right-click **Scope Options,** and from the resulting menu select **Configure Options.** The **Scope Options** page opens. Select the **Advanced** tab.



Vendor class: Alvarion

User class: Default User Class

Available Options	Description
☑ 002 Controller	List of Controllers IP Addresses

Server name:

IP address:

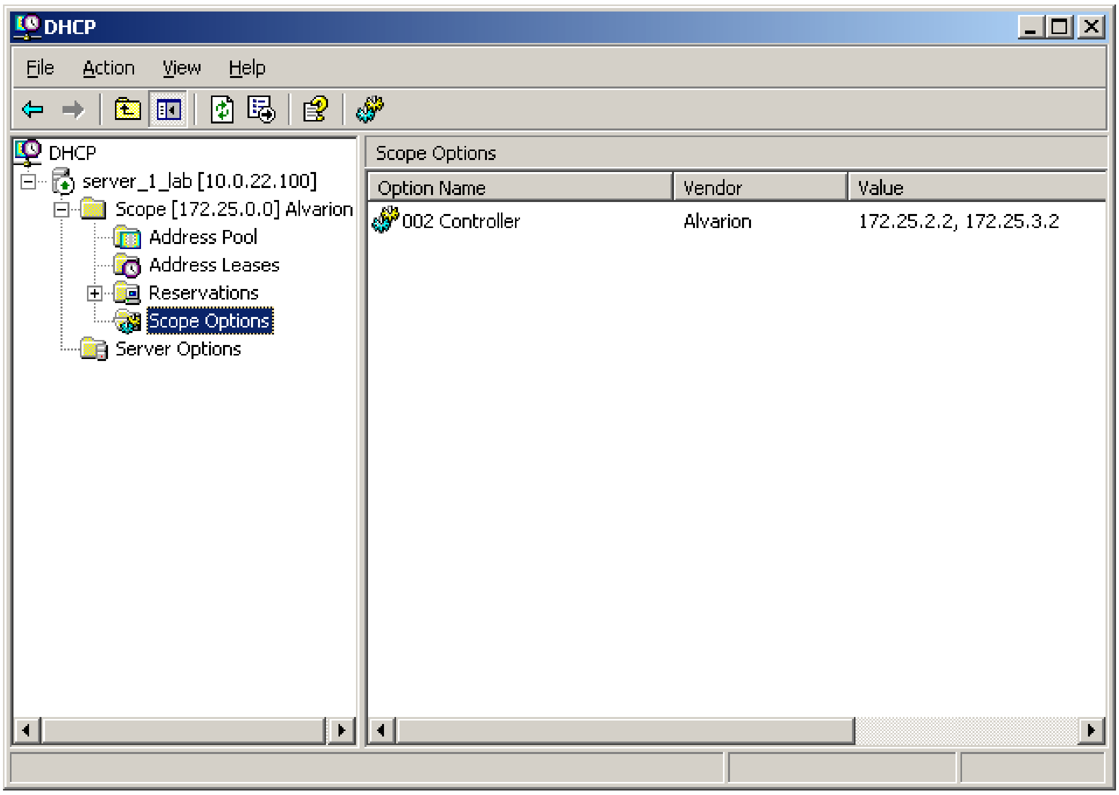
172.25.2.2
172.25.3.2

Figure C-5: Applying the Vendor Class

3 On the **Advanced** tab, configure the following:

- From the **Vendor class** drop-down menu, select **Alvarion.**
- Under **Available options,** enable the **001 Controller** checkbox.
- Under **IP address,** specify the IP address of the primary service controller in your network and select **Add.** Continue to build a list by specifying the IP addresses of all service controllers in your network, in descending order of importance.
- Select **OK.**

4 The service controller IP addresses now appear on the DHCP administration page under **Scope Options.** When an AP requests an IP address, these addresses are returned in a DHCP Ack message as option 43.



Option Name	Vendor	Value
002 Controller	Alvarion	172.25.2.2, 172.25.3.2

Figure C-6: DHCP Administration Page: Final

NOTE

For information about solving problems, see “Troubleshooting” on page 372.

C.2.4 ISC DHCP Server Configuration

This section shows you how to configure a Linux machine running an Internet Systems Consortium (ISC) DHCP server to use the Alvarion Ltd. vendor class. The procedure assumes that you have a Linux or Unix server that is running the ISC DHCP server.

For more information see the Linux Documentation Project’s “DHCP mini-HOWTO” at:
http://tldp.org/HOWTO/DHCP/index.html

You configure the ISC DHCP server by editing its configuration file; specifically, the main configuration file, */etc/dhcpd.conf*.

Following is a simple example of the */etc/dhcpd.conf* configuration file:

```
# dhcpd.conf
ddns-update-style ad-hoc;
option domain-name "alvarion.com";
option domain-name-servers 172.25.1.3;
default-lease-time 3600;

subnet 172.25.1.0 netmask 255.255.255.0 {
        range 172.25.1.100 172.25.1.150;
        option routers 172.25.1.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.1.255;

}
subnet 172.25.2.0 netmask 255.255.255.0 {
        range 172.25.2.100 172.25.2.150;
        option routers 172.25.2.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.2.255;
}
```

This sample file defines some general options to apply to all clients, as well as two DHCP Scopes—172.25.1.x and 172.25.2.x. You must add lines to the *dhcpd.conf* file to define the following for the ISC server:

- What the Alvarion vendor class identifier looks like

- What to return to the client when it sees that identifier

The following explains the changes that you must make to this sample file and the function of each added line.

- Create an option space called **Alvarion** and define a variable called **controller-address** within the space by adding the following lines.

  ```
  option space Alvarion;

  option Alvarion.controller-address code 1 = array of ip-address;
  ```

- Tell the server what to do when the client sends the vendor class identifier **Alvarion-AP** by adding the following lines. In this case you want the server to return the options defined in the Alvarion space that was created in the first step. Using the **vendor-option-space** command tells the server to return these values using DHCP option 43.

  ```
  if option vendor-class-identifier =  "Alvarion-AP" {

          vendor-option-space Alvarion;
  ```

```
}
```

- Specify the service controller IP addresses to return to the client by adding the following lines, where **172.25.2.2** and **172.25.3.2** are the specific IP addresses that you want returned. You can define this option globally or in one or more Scopes. You must define this option on all subnets from which an AP can potentially get an IP address. In this example only clients on the 172.25.1.x subnet get this option.

  ```
  option Alvarion.controller-address 172.25.2.2, 172.25.3.2;
  ```

Following is a revised sample configuration file that contains these additions, which appear in bold:

```
# dhcpd.conf
ddns-update-style ad-hoc;
option domain-name "alvarion.com";
option domain-name-servers 172.25.1.3;
default-lease-time 3600;

option space Alvarion;
option Alvarion.controller-address code 1 = array of ip-address;

if option vendor-class-identifier =  "Alvarion-AP" {
        vendor-option-space Alvarion;
}


subnet 172.25.1.0 netmask 255.255.255.0 {
        range 172.25.1.100 172.25.1.150;
        option routers 172.25.1.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.1.255;
        option Alvarion.controller-address 172.25.2.2, 172.25.3.2;

}

subnet 172.25.2.0 netmask 255.255.255.0 {
        range 172.25.2.100 172.25.2.150;
        option routers 172.25.2.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.2.255;
}
```

C.2.4.1 Troubleshooting

This section shows an Ethereal trace of a DHCP transaction, with the frames edited for readability. Four frames must be exchanged between the client and the server:

1. Client sends a `DHCP-Discover`
2. Server sends a `DHCP-Offer`

3. Client sends a `DHCP-Request`
4. Server sends a `DHCP-Ack`

The client sends its vendor class identifier in the `DHCP-Request` frame. The DHCP field of Frame 3 is expanded below.

The server sends the service controller addresses encapsulated as option 43 in the `DHCP-Ack` frame. Unfortunately the only way to decode these values is to look at the hexadecimal data. In this case the server returned the following 10 bytes:

```
2b 0a 01 08 ac 19 02  02 ac 19 03 02
```

which can be decoded as shown in the following table.

Segment	Value	Meaning
2b	43	DHCP option 43
0a	10	Field is 10 bytes long
01	01	Alvarion option code 1 as defined in the DHCP server
08	08	Option code 1 is 8 bytes long
ac 19 02 02	172.25.2.2	service controller IP addresses to return to the client
ac 19 03 02	172.25.3.2	

```
Frame 1 - DHCP-Discover

Frame 1 (346 bytes on wire, 346 bytes captured)
Ethernet II, Src: Alvarion_01:5f:05 (00:03:52:01:5f:05), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol


Frame 2 - DHCP-Offer

Frame 2 (346 bytes on wire, 346 bytes captured)
Ethernet II, Src: Cisco_23:0e:80 (00:0d:bc:23:0e:80), Dst: Alvarion_01:5f:05
(00:03:52:01:5f:05)
802.1Q Virtual LAN
Internet Protocol, Src: 172.25.1.1 (172.25.1.1), Dst: 172.25.1.201 (172.25.1.201)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol

Frame 3 - DHCP-Request

Frame 3 (346 bytes on wire, 346 bytes captured)
Ethernet II, Src: Alvarion_01:5f:05 (00:03:52:01:5f:05), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN
```

```
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4262bc18
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Alvarion_01:5f:05 (00:03:52:01:5f:05)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Request
    Option 54: Server Identifier = 172.24.50.4
    Option 50: Requested IP Address = 172.25.1.201
    Option 60: Vendor class identifier = "Alvarion-AP"
    Option 12: Host Name = "R054-00118"
    Option 55: Parameter Request List
    End Option
    Padding


Frame 4 - DHCP-Ack

Frame 4 (358 bytes on wire, 358 bytes captured)
Ethernet II, Src: Cisco_23:0e:80 (00:0d:bc:23:0e:80), Dst: Alvarion_01:5f:05
(00:03:52:01:5f:05)
802.1Q Virtual LAN
Internet Protocol, Src: 172.25.1.1 (172.25.1.1), Dst: 172.25.1.201 (172.25.1.201)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4262bc18
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 172.25.1.201 (172.25.1.201)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 172.25.1.1 (172.25.1.1)
    Client MAC address: Alvarion_01:5f:05 (00:03:52:01:5f:05)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP ACK
    Option 58: Renewal Time Value = 12 hours
    Option 59: Rebinding Time Value = 21 hours
    Option 51: IP Address Lease Time = 1 day
    Option 54: Server Identifier = 172.24.50.4
    Option 1: Subnet Mask = 255.255.255.0
    Option 3: Router = 172.25.1.1
    Option 15: Domain Name = "mgorr.local"
    Option 6: Domain Name Server = 172.24.50.4
    Option 43: Vendor-Specific Information (10 bytes)
    End Option
```

```
0000  00 03 52 01 5f 05 00 0d bc 23 0e 80 81 00 00 65   ..R._....#.....e
0010  08 00 45 00 01 54 81 68 00 00 ff 11 de 33 ac 19   ..E..T.h.....3..
0020  01 01 ac 19 01 c9 00 43 00 44 01 40 68 ec 02 01   .......C.D.@h...
0030  06 00 42 62 bc 18 00 00 00 00 00 00 00 00 ac 19   ..Bb............
0040  01 c9 00 00 00 00 ac 19 01 01 00 03 52 01 5f 05   ............R._.
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0110  00 00 00 00 00 00 00 00 00 00 63 82 53 63 35 01   ..........c.Sc5.
0120  05 3a 04 00 00 a8 c0 3b 04 00 01 27 50 33 04 00   .:.....;...'P3..
0130  01 51 80 36 04 ac 18 32 04 01 04 ff ff ff 00 03   .Q.6...2........
0140  04 ac 19 01 01 0f 0c 6d 67 6f 72 72 2e 6c 6f 63   .......mgorr.loc
0150  61 6c 00 06 04 ac 18 32 04 2b 0a 01 08 ac 19 02   al.....2.+......
0160  02 ac 19 03 02 ff                                 ......
```